HZD

Hessische Zentrale für Datenverarbeitung

HESSEN

TRENDBERICHT **2017**

VORWORT

Technologietrends können Emotionen hervorrufen. Sie können lange Warteschlangen vor den Läden der Hersteller entstehen lassen oder als „Hype" die einschlägigen Medien, Konferenzen oder Fachgespräche beherrschen. Sie können aber auch kontrovers diskutiert werden – etwa wenn es um ihre markt- oder sicherheitspolitischen Auswirkungen geht.

Im vorliegenden Trendbericht versuchen wir wieder, IT-Trends jenseits von Euphorie oder Aufgeregtheit zu beschreiben und ihre möglichen Auswirkungen auf die öffentlichen Verwaltungen zu analysieren. Dies hilft uns dabei, die Verwaltungsarbeit in einer zunehmend digitalisierten Gesellschaft langfristig zu unterstützen und moderne IT-Dienstleistungen für unsere Kunden zu erbringen.

Wesentliche Rahmenbedingungen für unsere Arbeit werden außerhalb der HZD bestimmt. Neben IT-Trends und der allgemeinen Digitalisierung sind dies vor allem die politischen Rahmenbedingungen, die in der Strategie Digitale Verwaltung Hessen 2020, der Strategie Digitales Hessen oder dem künftigen E-Government-Gesetz ihren Ausdruck finden. Aber auch IT-Programme z. B. der Justiz, des Finanzressorts oder rund um das Verwaltungsportal schaffen neue Möglichkeiten, moderne Lösungen und wichtige IT-Trends im digitalen Arbeitsplatz einer leistungsstarken Verwaltung zusammenfließen zu lassen.

Nicht alle IT-Trends führen zu Veränderungen, die dem Anwender unmittelbar ins Auge fallen. Schnellere und energiesparende Technik, neue Rechnerarchitekturen oder Software-definierte

// Moderne und beständige IT-Lösungen erfordern klare Rahmenbedingungen.

IT-Landschaften tragen eher im Hintergrund dazu bei, IT-Verfahren besser, schneller und sicherer bereitstellen zu können. So nutzen wir Entwicklungen der Informations- und Kommunikationstechnik sowohl bei der internen Optimierung unserer Arbeit als auch zur Verbesserung der Lösungen für unsere Kunden. Die entstehenden Potenziale zu erschließen, ist unsere gemeinsame Aufgabe.

***Joachim Kaiser**, Direktor der HZD*

EINLEITUNG

Nur wenige Entwicklungen in der IT sind in der Lage, die digitale Welt grundlegend zu verändern. Disruptive Innovationen, die zunächst in einer Marktnische entstehen, benötigen i. d. R. einige Zeit sich so zu entwickeln, dass sie etablierte Techniken bzw. Anbieter verdrängen können. Eine Technologie, die dieses Potenzial hat, ist die Blockchain (S. 10). Sie ist das informationstechnische Fundament für Kryptowährungen (S. 15), die die Geschäftsmodelle klassischer Banken in Frage stellen. Eine andere grundlegende Veränderung besteht in der Art, wie wir das Internet nutzen. Die zunehmend stärkere Vernetzung von vermeintlich intelligenten Dingen stellt wesentlich höhere Anforderungen an Geschwindigkeit und Sicherheit im Netz, als wenn klassische Inhalte übertragen werden: Das „fühlende" Netz (S. 25) beflügelt daher eine ganze Reihe weiterer Techniken, die im Hintergrund arbeiten (s. Kap. II) oder in der virtuellen und angereicherten Realität (S. 19) einen Eindruck davon vermitteln, wie die Digitalisierung verschiedenste Lebensbereiche durchdringen kann.

Die zunehmende Digitalisierung der Welt birgt neue Chancen, bringt aber auch neue Herausforderungen mit sich. Nicht nur massive Angriffe auf informationstechnische Infrastrukturen werfen die Frage nach staatlicher Regulierung auf. Auf europäischer Ebene wurde diesem Umstand mit zwei neuen Verordnungen Rechnung getragen, die den Datenschutz (S. 52) und den Umgang mit elektronischer Identifizierung (S. 57) regeln. Doch staatliche Regulierung allein reicht nicht aus, den Cyberspace – und unsere Daten – sicherer zu machen. Einen möglichen Ansatz, wie auch Privatpersonen dazu beitragen können, zeigt die Volksverschlüsselung (S. 53). Die Daten von Privatpersonen, Unternehmen und Behörden stellen neben Kryptowährungen ein weiteres elektronisches und werthaltiges Gut dar und werden daher auch als „Währung der Informationsgesellschaft" bezeichnet. Aus ihnen Nutzen zu ziehen, ist Gegenstand ganz unterschiedlicher Techniken (s. Kap. III).

Neben Technik, Finanzen und Daten sind es vor allem die Menschen, die die Informationsgesellschaft prägen. Wertvolle Beiträge zu diesem Trendbericht lieferten mit ihrem Wissen Susanne Alberts, Heidrun Bechtold, Harms Becker, Gundula Bucsa, Matthias Guckler, Claudia Iske-Nikolay, Markus Keutner, Dr. Alberto Kohl, Birgit Lehr, Suse Märkle, Manuel Milani, Peter Müller, Uwe Pörschke, Markus Schramm, Skadi Stephan und Friederike van Roye.

Wir hoffen, dass der vorliegende Trendbericht für unsere Leserinnen und Leser ein Gewinn ist, und würden uns über Feedback zu dieser Ausgabe freuen.

Dr. Markus Beckmann

ZU DIESEM TEXT

Mit dem Trendbericht ermöglichen wir unseren Leserinnen und Lesern einen Ausblick auf aktuelle Trends in der Informationstechnologie. Dabei wollen wir uns jedoch nicht auf eine rein fachliche Information über die technischen Hintergründe und die weitere Entwicklung beschränken. Als IT-Gesamtdienstleister für die Hessische Landesverwaltung steht für uns die strategische Bedeutung der erfassten Trends für die Verwaltung im Mittelpunkt. Daher haben wir jedes einzelne Thema im Hinblick auf seine Auswirkungen auf die Verwaltung bewertet. Der Fokus liegt dabei auf der Hessischen Landesverwaltung. Neben einem kurzen Bewertungstext werden jeweils drei Kennzahlen angegeben, die die Einordnung der Themen in IT-strategische Überlegungen erlauben.

Verwaltungsrelevanz

Die Verwaltungsrelevanz gibt an, in welchem Maß sich ein Trend auf die Verwaltung auswirken kann. Dies kann auf zweierlei Art erfolgen: Zum einen können Trends zu technischen Änderungen in der IT-Landschaft führen bzw. solche Änderungen ermöglichen. Diese Trends sind daher in dem Maß verwaltungsrelevant, wie sie sich auf einige oder alle IT-Arbeitsplätze im Land auswirken – entweder direkt am Arbeitsplatz oder durch die Gesamtinfrastruktur.

Zum anderen können IT-Trends dazu führen, dass sich Verwaltungsabläufe ändern oder ganz neue Abläufe etabliert werden (können). In diesen Fällen haben die IT-Trends also Auswirkungen auf die Kernprozesse der Verwaltung.

Die Verwaltungsrelevanz wird auf einer fünfteiligen Skala angegeben, in der die Auswirkung des Trends auf die Verwaltung bewertet sind:

■■■■	starke
■■■□	deutliche
■■□□	mittlere
■□□□	geringe
□□□□	keine

Marktreife/Produktverfügbarkeit

Der Wert für Marktreife bzw. Produktverfügbarkeit gibt an, wie lange es dauern wird, bis Produkte, die auf der im Trend beschriebenen Entwicklung basieren, am Markt verfügbar sind. Die fünfteilige Skala gibt die Marktreife bzw. Produktverfügbarkeit mit folgenden Werten an:

■■■■	sofort
■■■□	1–2 Jahre
■■□□	2–4 Jahre
■□□□	mindestens 4 Jahre
□□□□	noch nicht absehbar

Umsetzungsgeschwindigkeit

Die Umsetzungsgeschwindigkeit gibt an, wie schnell ein Trend in der Verwaltung umgesetzt werden kann. Sie kann als ein Maß für die Komplexität der entsprechenden Trendergebnisse gesehen werden: Je komplizierter ein Resultat oder Produkt ist, desto länger dauert es, dieses in Verwaltung und Unternehmen nutzbar zu machen. Die fünfteilige Skala gibt die Einführungsgeschwindigkeit mit folgenden Werten an:

■■■■	sofort
■■■□	1–2 Jahre
■■□□	2–4 Jahre
■□□□	mindestens 4 Jahre
□□□□	noch nicht absehbar

INHALT

01

ARCHITEKTUREN // LÖSUNGEN // SYSTEME

01

KETTENREAKTION – BLOCKCHAIN

Für die einen ist sie eine Revolution in der Bankenwelt. Die anderen wissen noch nicht, ob sie Chance oder Bedrohung für den Finanzsektor ist. Aber die meisten fragen sich wohl, ob mehr dahinter steckt als nur ein neuer Hype. Die Rede ist von der sog. Blockchain, einem informationstechnischen Mechanismus, der mit viel Kryptografie und großer Transparenz das Rückgrat von elektronischen Währungen wie Bitcoins oder Ethereum ist (s. Artikel „Kryptowährung"). Auch wenn die Verbindung zwischen Blockchain und Kryptowährungen sehr eng ist, ermöglicht dieser Mechanismus mehr als einfaches elektronisches Bezahlen. Die Grundidee hinter der Blockchain besteht darin, elektronische Transaktionen von Werten

- unmittelbar, d. h. ohne zentrale Verwaltung,
- sicher und
- schnell

zu ermöglichen. Solche Werte sind im ökonomischen Sinn Güter, also Waren und Dienstleistungen, oder Forderungen, etwa Geld und andere Finanzierungsinstrumente. Während bei einem klassischen Kauf die Beteiligten – Käufer und Verkäufer – mit ihren Werten direkt zusammenkommen und das Geschäft tätigen, ist dies beim Versandhandel nicht der Fall. Hier hat es sich bewährt, für die Übermittlung von Gütern und Forderungen Treuhänder einzuspannen. Das sind einerseits die Post und Zustelldienste, andererseits Banken und Zahldienste. Ein Treuhänder ist bevollmächtigt, fremde Rechte auszuüben, und genießt daher auch das Vertrauen der Geschäftspartner. Beim Handel mit elektronischen Gütern wie Software kann einer der Treuhänder entfallen, nämlich derjenige, der für die Übermittlung des Gutes zuständig ist. Er wird durch „das Netz" ersetzt. Das Bezahlen solcher Güter ist aber noch immer an Banken gekoppelt – entweder über deren Online-Plattformen oder über andere Bezahldienste, die ihrerseits das Bankenwesen nutzen. Diesen vermeintlich unumgänglichen Treuhänder zu ersetzen, ist ein Ziel des Blockchain-Modells.

// In 2014 wurde die Gesamtrechenleistung des Bitcoin-Netzwerks auf über 200 Exa-FLOPS = 200 x 1018 Gleitkommaoperationen pro Sekunde geschätzt. Der derzeit schnellste Superrechner Sunway TaihuLight erreicht 0,093 ExaFLOPS.

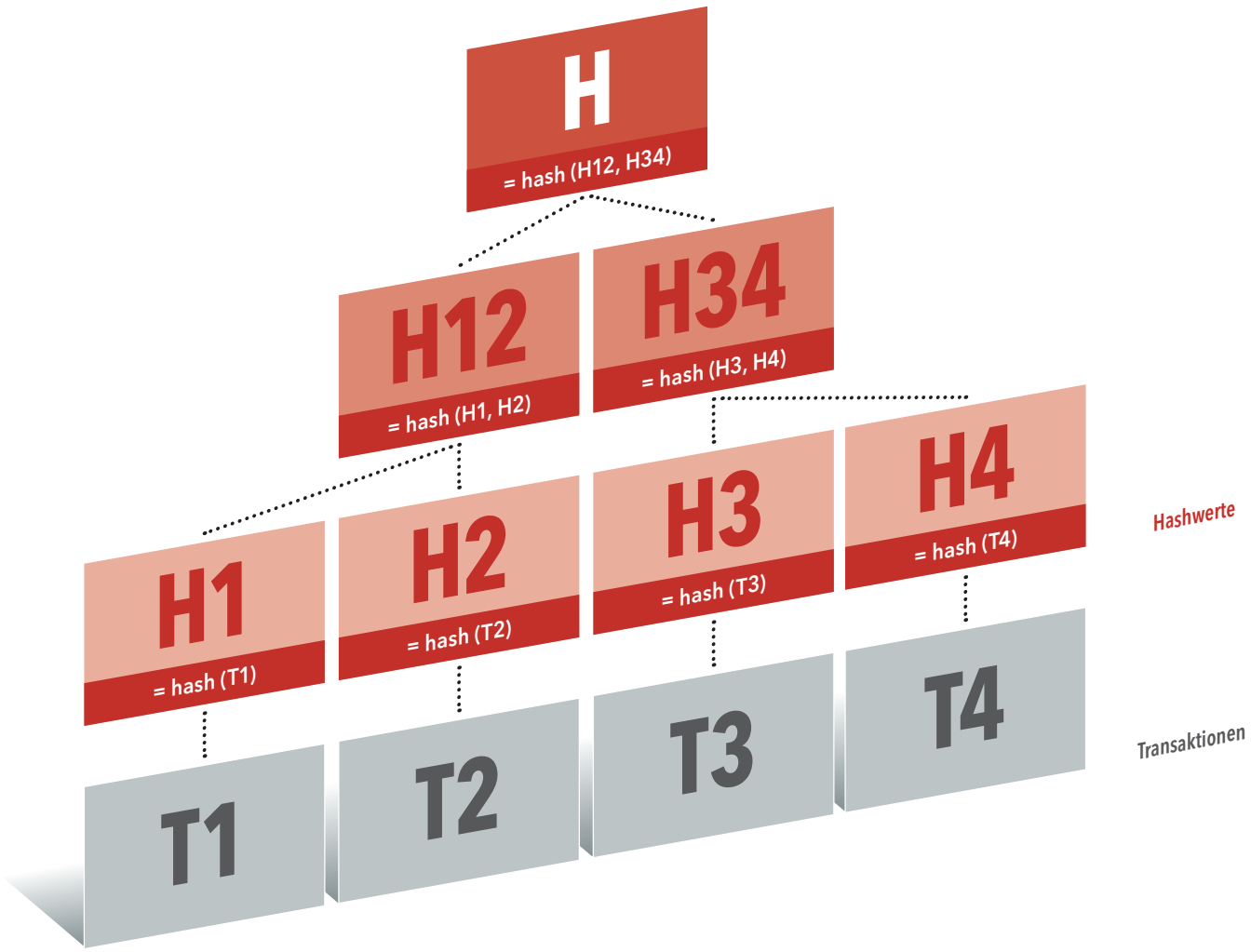
Stark vereinfacht gesagt ist die Blockchain eine öffentliche elektronische Liste von Transaktionen, die grundsätzlich von jedem erweitert werden kann. D. h. es gibt keine ausgezeichnete Instanz, die darüber entscheidet, was „in den Büchern" steht, oder nicht. An deren Stelle tritt ein Verfahren, das im Konsens die Aufnahme neuer Transaktionen regelt. Jeder, der über einen Rechner mit Netzzugang verfügt, kann sich an diesem Verfahren beteiligen.

Blockbildung

Wenn das Modell auch Transaktionen mit geringem Wert zulässt, können ggf. sehr viele Transaktionen zusammenkommen. Eine entsprechende Liste würde also sehr schnell wachsen. Daher organisiert man beim Blockchain-Modell die Transaktionen in Gruppen und bindet sie *en bloc*, eben als Block, in die Liste ein. Diese Arbeit – das Bauen und Einbinden der Blöcke – kann grundsätzlich jeder Rechner übernehmen – auch wenn in der Praxis eine immense Rechenleistung erforderlich ist, um die anfallenden kryptografischen Aufgaben zu lösen (s. linke Spalte).

Damit ist die Forderung nach einem Verfahren ohne zentrale Verwaltung erfüllt. Wie aber sieht es mit Sicherheit und Schnelligkeit aus?

Ein Aspekt der Sicherheit beim Blockchain-Modell besteht in der Transparenz des Verfahrens. Das mag auf den ersten Blick verwundern. Es wird aber verständlich, wenn man bedenkt, dass Fakten, die öffentlich bekannt sind, nicht durch einfache Behauptungen abstreitbar sind. Die Transparenz des Verfahrens ergibt sich daraus, dass die wesentlichen Daten der Transaktion offenliegen. Auf verschiedenen Internetsei-

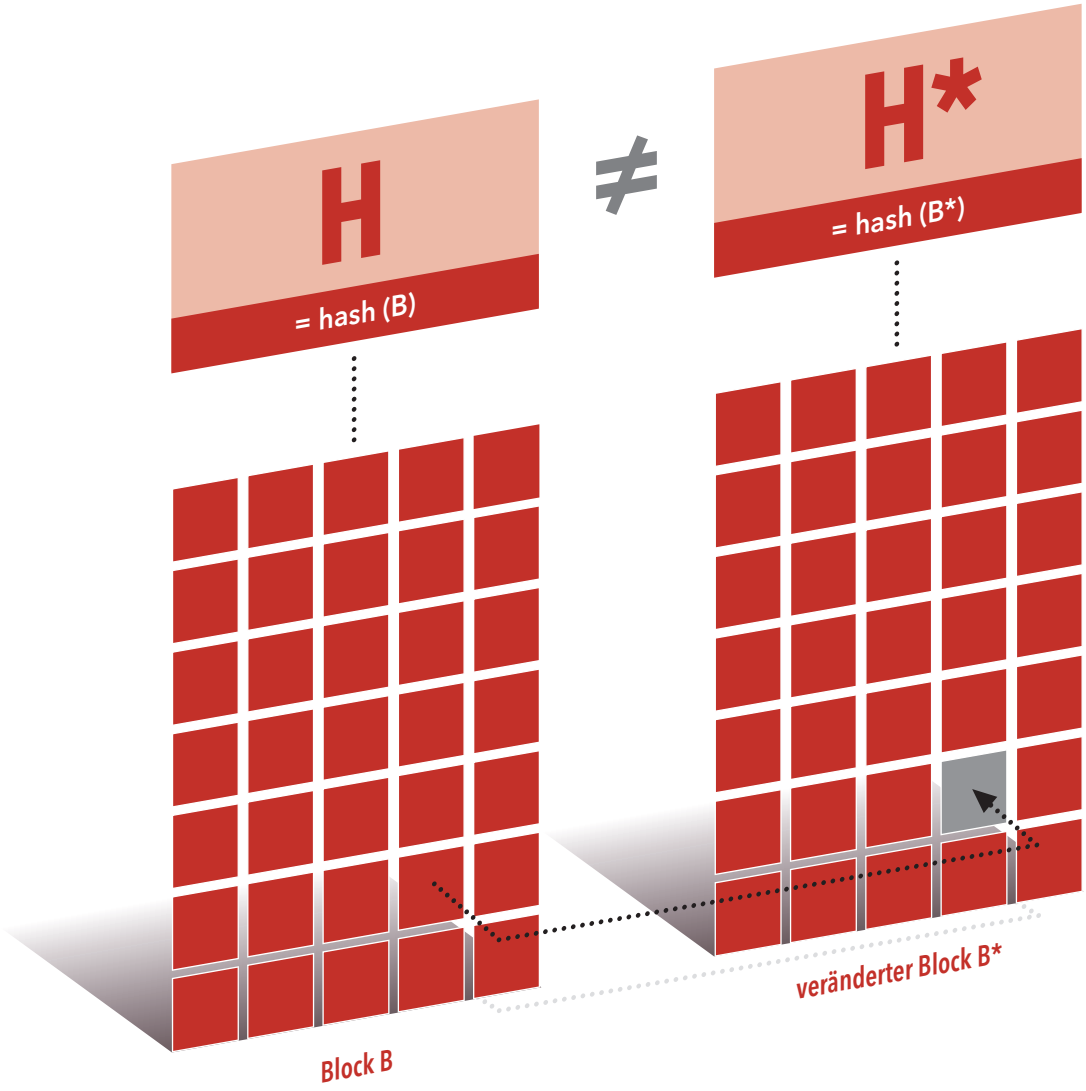


ten kann man z.B. „live" verfolgen, wie Bitcoins ihre Besitzer wechseln. Allerdings ist dort auch nicht mit Klarnamen zu sehen, wer an einer Transaktion beteiligt ist. Stattdessen findet man zufällig aussehende Zeichenfolgen vor. Darin zeigt sich ein weiterer Sicherheitsmechanismus des Blockchain-Modells: die Codierung von Informationen mit Hilfe von Hashfunktionen.

Hashfunktionen sind – einfach gesagt – Abbildungen von beliebigen Texten oder Daten auf Zeichenfolgen einer bestimmten Länge. Diese Funktionen sind so konstruiert, dass effizient zu berechnen ist, welche Zeichenfolge zu einem gegebenen Ausgangstext gehört. Zu einem vorgegebenen Hashwert einen Ausgangstext zu finden, der gerade auf diesen Hashwert abgebildet wird, soll aber „unendlich schwierig" sein. Deshalb nennt man solche Funktionen auch Einwegfunktionen. Das „unendlich schwierig" bedeutet dabei, dass es keinen Weg geben darf, der wesentlich schneller ist, als alle möglichen Ausgangstexte durchzuprobieren, und dass selbst mit größter Computerleistung das Durchprobieren „unendlich" lange dauern würde.

Beispiele für Hashfunktionen, die im Zusammenhang mit Blockchains eingesetzt werden, sind RIPEMD-160 und SHA-256, die Hashwerte mit 160 resp. 256 Zeichen erzeugen.

01



Durch die Veränderung eines Teils der Daten im Block ändert sich dessen Hashwert.

Hashwerte

Hashfunktionen werden beim Aufbau der Blockchain nicht nur dazu verwendet, einzelne Teilinformationen zu den Transaktionen kryptografisch zu verschlüsseln. Auch für jede Transaktion, die in einem Block gespeichert werden soll, wird der Hashwert berechnet. Doch damit nicht genug: Aus Paaren dieser Hashwerte werden wiederum jeweils neue Hashwerte berechnet, sodass eine baumartige Struktur von Hashwerten, ein sog. Merkle-Baum, entsteht (s. Abbildung). Kryptografische Hashfunktionen sind so konstruiert, dass kleine Änderungen in den Ausgangsdaten zu einem wesentlich anderen Hashwert führen. Somit lässt sich anhand des Hashwertes schnell erkennen, wenn Daten verfälscht wurden.

Verkettung

Der Name Blockchain deutet darauf hin, dass darin die Blöcke verkettet werden („chain" engl. für „Kette"). Und tatsächlich wird – ausgehend von einem Startblock – in jedem neuen Block vermerkt, welcher Block der vorhergehende ist.

Dazu wird dessen Hashwert im neuen Block notiert – vergleichbar einer Adresse oder Telefonnummer. Ein solcher Verweis auf Daten mittels eines Hashwertes heißt Hashpointer („pointer" engl. für „Zeiger"). Hashwerte, die nur auf den Daten eines Blocks basieren, als Verweise zu benutzen, hat den Vorteil, dass diese Art der Referenz unabhängig vom Ort der Daten-Aufbewahrung ist. Das unterstützt das Ziel einer dezentralen Verwaltung von Transaktionen.

Geschwindigkeit

Bleibt noch das Ziel einer schnellen Abwicklung der Transaktionen. Auch wenn die Hashfunktionen wohldefiniert sind, ist ihre Berechnung durchaus aufwändig. Kreditkartenunternehmen und andere Zahlungsdienste sind in der Lage, zehntausende Transaktionen pro Sekunde durchzuführen. Der Anspruch an ein Blockchain-basiertes Verfahren nicht langsamer zu sein, als die in der jeweiligen Branche üblichen Dienste, liegt auf der Hand. Entsprechende Zielvorgaben für das Einbinden einer Transaktion in die Blockchain betreffen damit zunächst die technische Transaktionsabwicklung. Aber auch die Organisation spielt in puncto Geschwindigkeit eine Rolle: Durch die unmittelbare Beziehung zwischen den Beteiligten vergeht für die Wertstellung der Transaktion keine durch zwischengeschaltete Akteure begründete Bearbeitungszeit, wie etwa bei der Abwicklung von Zahlungen durch Banken.

Revolution?

Bis hier sind grundlegende Elemente des Blockchain-Modells beschrieben, die eine sichere, schnelle und unmittelbare Abwicklung von elektronischen Transaktionen ermöglichen. Aber diese begründen wohl kaum eine Revolution im Internet und im Bankengeschäft. Warum das Blockchain-Modell trotzdem so viel Aufmerksamkeit – sowohl in der Geschäftswelt als auch in der IT – erfährt, erschließt sich erst, wenn man einen genaueren Blick auf die Transaktionen wirft.

Transaktionen

Diese bestehen im Wesentlichen aus Informationen zu den Eingangsdaten (Input) und Ausgangsdaten (Output) sowie einigen weiteren Informationen (Metadaten), wie etwa dem Hashwert der Transaktion oder der Anzahl der Inputs bzw. Outputs. Jeder Input einer Transaktion ist Output einer früheren Transaktion. Es lassen sich jedoch durch Transaktionen mehrere Werte zusammenfassen oder auch Werte verteilen.

So wird zu jedem Input vermerkt, aus welcher früheren Transaktion (über deren Hashwert) er stammt und der wievielte Output er dort war. Dazu kommt eine Hash-Referenz auf die Signatur des ursprünglichen Besitzers, der den Wert für die neue Transaktion freigeben muss. Zu jedem Output wird neben dem Wert – z. B. dem Betrag – per Hashwert vermerkt, wer der Empfänger ist. Soweit klingt alles sehr einfach und strukturiert. Auch hier findet sich noch nichts Revolutionäres. Doch es gibt noch weitere Informationen in den Transaktionen. Zu den Inputs und Outputs können kleine Skripte gespeichert werden, die den genauen Ablauf der Transaktion steuern. Damit lässt sich z. B. das Auslösen einer Transaktion bis zu einem bestimmten Zeitpunkt hinauszögern. Oder es kann festgelegt werden, dass die Transaktion nur dann ausgelöst wird, wenn eine bestimmte Zahl von Beteiligten den Vorgang signiert hat. Damit lässt sich z. B. eine dritte Person als Treuhänder in ein Verkaufsgeschäft einbinden, die im Streitfall entscheidet, ob der Verkäufer zu bezahlen ist, oder ob der Käufer sein Geld zurückbekommt. Im ersten Fall wird die Transaktion an den Verkäufer ausgeführt, wenn er und der Treuhänder sie signieren. Im zweiten Fall wird die entsprechende Transaktion von Käufer und Treuhänder signiert und damit ausgelöst.

Was sich alles mit diesen Skripten abwickeln lässt, hängt von der verwendeten Skriptsprache ab. Diese umfasst z. B. im Falle der Kryptowährung Bitcoin 256 mögliche Anweisungen – von einfachen Zuweisungen bis hin zur Überprüfung mehrerer Signaturen. Sie ermöglicht aber z. B. keine Programmierung von Schleifen. Andere Blockchain-Modelle verwenden mächtigere Sprachen, z. B. die Sprache Solidity der Ethereum-Plattform.

Smart Contracts

Damit sind vier wesentliche Facetten des Blockchain-Modells beschrieben: Es ermöglicht

- wertvolle Transaktionen durchzuführen,
- deren Abwicklung durch kryptografischen Schutz und Transparenz abzusichern,
- die Geschäfte auf die unmittelbar Beteiligten zu beschränken und
- komplexe Handlungsmodelle schnell und nachvollziehbar umzusetzen.

Blockchains sind daher eine Implementierung von cleveren Verträgen, sog. Smart Contracts. Der Begriff wurde 1994 von dem Computerwissenschaftler und Juristen Nick Szabo geprägt. Zu seinen Zielen für Verträge, die sich selber ausführen, gehörten wirtschaftliche Gesichtspunkte wie etwa die Reduktion von Kosten für Schlichtung oder Vollstreckung. Aber auch höhere geschäftliche Sicherheit und reduzierter Bedarf an beteiligten Dritten standen schon 14 Jahre vor Blockchain und Bitcoins auf seiner Agenda.

Anwendungen

Als eine stark vereinfachte Anwendung von Smart Contracts nennt Szabo die Bezahlterminals für das bargeldlose Einkaufen, den automatisierten Transfer standardisierter Geschäftsdaten (EDI) oder die Zuteilung von Bandbreiten mit Hilfe von automatisierten Marktplatz-Systemen. Auch Systeme für die digitale Rechteverwaltung (engl. Digital Rights Management, DRM) werden gelegentlich als Anwendungen von Smart Contracts genannt.

Derzeit wird das Thema Blockchain zumeist in enger Verbindung mit Kryptowährungen betrachtet. Die Entwicklung einer solchen universellen Währung ist sicher nicht Aufgabe einer öffentlichen Verwaltung. Jedoch können Verwaltungen solche Währungen als Zahlungsmittel akzeptieren, wie es eine Stadt in der Schweiz erstmalig getan hat. Daneben gibt es Überlegungen zu Anwendungen von Blockchains jenseits reiner Bezahlvorgänge, die für die öffentlichen Verwaltungen zumindest als Denkmodelle dienen können. So planen die Staaten Honduras und Georgien jeweils, ihre Grundbücher in einer Blockchain abzulegen. Und schließlich könnte ein Blockchain-Modell sowohl die automatische, skriptgesteuerte Bereitstellung von IT-Leistungen in Software-definierten Umgebungen – inklusive deren Abrechnung – auch in der Verwaltungs-IT steuern.

Sicherheit (der Verfahrens)

Blockchains verwenden viel Kryptografie und Transparenz, um die Daten und Verarbeitung sicher zu machen. Trotzdem ist im Zusammenhang mit Kryptowährungen von verschiedenen Pannen oder auch kriminellen Manipulationen zu hören. Und nicht zuletzt die Verwendung von Kryptowährungen auf den dubiosen elektronischen Marktplätzen für illegale Güter rückt auch das Blockchain-Modell in ein zweifelhaftes Licht. Betrachtet man die Problemfälle etwas genauer, stellt man fest, dass nur wenige davon in den Mechanismen der betroffenen Blockchain begründet waren. In einem Fall wurden tatsächlich die im Modell der Ethereum-Plattform implementierten Möglichkeiten und konzeptionellen Schwachstellen genutzt, um virtuelles Geld zu „entwenden". Dies führte zu einer schwerwiegenden Korrektur, einem sog. „hard fork", in der zugehörigen Blockchain. Die anderen Vorfälle betreffen im Kern die Schnittstelle zwischen „realer" und „virtueller" Welt. Ein Angriffspunkt sind dabei die Einrichtungen, in denen Nutzer der Blockchain den Zugriff auf ihre Werte und die zugehörigen Schlüssel verwalten. Zunächst müssen Nutzer in den Besitz virtueller Werte gelangen. Im Bitcoin-Modell können sie die virtuelle Währung als Gegenleistung für das „Schürfen" – also das Berechnen gültiger Hashwerte – erhalten. Wer diese Möglichkeit nicht hat, kann Bitcoins gegen reale Währungen eintauschen. Der Wechselkurs kann auf verschiedenen Finanzportalen verfolgt werden.

Auch wenn der Besitz von virtuellen Werten in der Blockchain dokumentiert ist, erfolgen deren An- und Verkauf bzw. der Handel damit über Anwendungen, die i.d.R. mit üblichen Sicherheitsmechanismen geschützt sind. Die entsprechenden Börsen und Marktplätze sind nicht selten Webanwendungen und die Betreiber nur bedingt Finanzspezialisten. So resultierten verschiedene Sicherheitsvorfälle bei Kryptowährungen auf internen oder externen Angriffen auf diese Plattformen und weniger auf Fehlern im implementierten Blockchain-Modell. Auch

die Eignung von virtuellen Werten für den Handel mit illegalen Gütern hängt nur bedingt am Blockchain-Mechanismus selber, denn hier lassen sich ja aufgrund der Transparenz sämtliche Transaktionen anhand von Pseudonymen nachvollziehen. Die Attraktivität von Kryptowährungen für illegale Geschäfte hängt vielmehr davon ab, welche Maßnahmen zur Anonymisierung bzw. zur Verschleierung von Identitäten beim An- und Verkauf von Werten ergriffen werden können.

Bewertung

Blockchains sind ein sehr interessantes Modell, wenn es darum geht, den Transfer von virtuellen Werten neu zu gestalten. In einigen Bereichen hat diese schnelle, sichere und unmittelbare Art der Abwicklung von Transaktionen sicher das Zeug, den Handel mit Gütern und Dienstleistungen zu revolutionieren. Doch jeder Ansatz von Revolution weckt auch immer den Ruf nach vermehrter Regulierung. Hier kommt es im Einzelfall darauf an, wie frei der neue Weg beschritten werden kann. Für den Einsatz von Blockchains in der öffentlichen Verwaltung spielen zwei Aspekte eine wesentliche Rolle. Der eine betrifft die Art der Werte, die verarbeitet werden. Welche Güter und Dienstleistungen werden transferiert? Sind dies virtuelle oder reale Güter? Können das auch Urkunden, die etwa das Eigentum von Land begründen (s. o.), oder Bescheide sein? Stehen diesen Gütern „lediglich" finanzielle Forderungen gegenüber?

Zum anderen haben die Beteiligten, und damit die Schnittstellen zwischen „realer" Verwaltungswelt und ihrem virtuellen Pendant in der Blockchain, besondere Bedeutung. Die ergibt sich zunächst aus der Frage, ob allein Verwaltungsstellen die Blockchain nutzen, oder ob auch Verwaltungskunden zu beteiligen sind. Sofern man sich mit dem Modell in einer geschlossenen Anwenderwelt bewegt, kann man die Regeln der Nutzung selbständig festlegen. Andernfalls ist die Rechtsverbindlichkeit der Transaktionen zu bewerten.

Eine Revolution der Verwaltung wird die Blockchain wohl kaum auslösen. Die in dem Modell vereinten Techniken können aber dazu beitragen, dass sich Gewohnheiten im Umgang mit Daten und Verwaltungsverfahren verändern.

BLOCKCHAIN

Verwaltungsrelevanz:

■□□□

Umsetzungsgeschwindigkeit:

■■□□

Marktreife/Produktverfügbarkeit:

■■■■

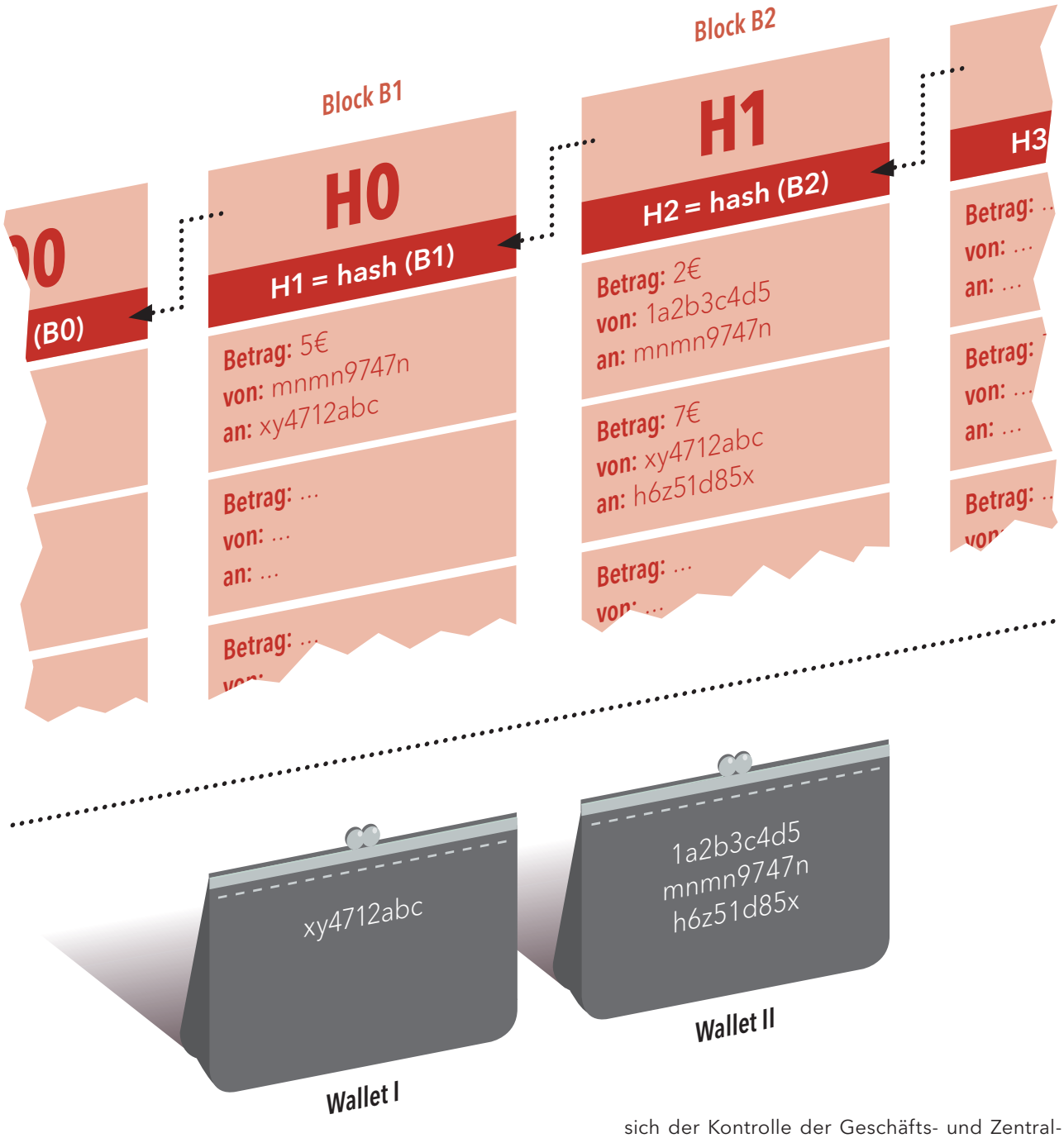
KRYPTOWÄHRUNGEN

Eine Kryptowährung ist ein digitales Zahlungsmittel, das verteilt und dezentral verwaltet wird und durch die Verwendung kryptographischer Methoden abgesichert ist. Eine solche Währung zu nutzen erfordert kein Konto bei einer Bank, gegen das Buchungen von Bargeld oder elektronische Werte verrechnet werden, denn hier werden nicht die Zahlungsvorgänge eines einzelnen Nutzers dokumentiert. Stattdessen findet die Buchführung sämtlicher Transaktionen in einer allen Nutzern zugänglichen Datenbank (engl. „ledger") statt.

Das digitale Geld wird von verschiedenen Akteuren dezentral erzeugt („geschürft") bzw. zwischen ihnen transferiert, und die anfallenden Daten werden verteilt gespeichert. Daher ist es

// Da bei Kryptowährungen die anfallenden Daten verteilt gespeichert werden, muss jeder einzelne Vorgang so abgesichert werden, dass er zum einen nicht verfälscht werden und zum anderen nicht verloren gehen kann.

notwendig, jeden einzelnen Vorgang derart abzusichern, dass er zum einen nicht verfälscht werden und zum anderen nicht verloren gehen kann. Der wesentliche Mechanismus, der kryptografische Währungen sowohl dezentralisiert als auch sichert, ist die Blockchain (s. Artikel



„Kettenreaktion – Blockchain"). Durch ihn benötigen Kryptowährungen keine zentrale Organisation, die über die Menge des verfügbaren „Geldes" oder die Korrektheit der Transaktionen wacht. So entsteht ein Finanzmarkt, der sich der Kontrolle der Geschäfts- und Zentralbanken – und damit zunächst auch der Staaten – entzieht. Dies hat zum einen den Ruf nach staatlicher Regulierung laut werden lassen. Zum anderen haben auch Banken begonnen, eigene Kryptowährungen – mit zentraler Steuerung – zu entwickeln, um von dieser Form des Geldgeschäftes profitieren zu können. So

haben z. B. vier Großbanken ein entsprechendes Projekt aufgesetzt, aber auch die britische Zentralbank arbeitet an dem Thema.

Die derzeit am meisten beachtete und genutzte Kryptowährung ist die Bitcoin. Ihre Marktkapitalisierung – also der Gegenwert der in Umlauf befindlichen Anteile – beträgt rund 11 Milliarden Euro und liegt damit weit höher als die der zweitplatzierten Kryptowährung Ether, die über die Plattform Ethereum verwaltet wird. Diese kommt auf knapp 850 Millionen Euro. Es gibt inzwischen einige hundert Kryptowährungen, die in öffentlichen Listen genannt werden. Deren Top-100 haben insgesamt einen Gegenwert von rd. 13 Milliarden Euro. Dies unterstreicht die Bedeutung der Bitcoin, die rd. 85% dieses Wertes für sich verbucht. Trotzdem sind auch die kleineren (Plätze 50–100) jeweils noch mit 750 Tsd. bis zu drei Millionen Euro bewertet.

Handhabung

„Das Geld der kryptografischen Währung wird in einem virtuellen Geldbeutel aufbewahrt", könnte man denken. Tatsächlich existieren die Werte jedoch lediglich in der Blockchain. Dort werden sie durch Transaktionen ihrem jeweiligen Besitzer – identifiziert über dessen öffentlichen kryptografischen Schlüssel – zugewiesen. Und nur der jeweilige Besitzer kann seine Werte – mit Hilfe eines geheimen Schlüssels – weitergeben. Diese Schlüssel sind es, die in den virtuellen Geldbeuteln (engl. „wallet") verwaltet werden.

Bei manchen kryptografischen Währungen, z. B. Bitcoin, kann man virtuelles Geld als Gegenleistung für erfolgreiches Schürfen erhalten. Dieser Vorgang erfordert aber inzwischen eine sehr hohe Rechenleistung, die nur noch von Rechenzentren zu bewältigen ist. Ein anderer Weg zum Erwerb virtuellen Geldes besteht im Umtausch gegen „reale" Währungen bei Online-Börsen oder bei Privatpersonen. Hier erhalten Nutzer gegen Zahlung beispielsweise von Euro-Beträgen eine entsprechende Menge virtuellen Geldes an ihren kryptografischen Schlüssel transferiert.

Online-Börsen und virtuelle Wallets sind kritische Stellen für die sichere Nutzung von kryptografischen Währungen. Der hohe kryptografische Schutz der Währung sichert zwar die einzelnen Transaktionen und ihre Gesamtheit in der Blockchain ab. Er schützt aber nicht davor, dass ein Angreifer Schlüssel aus einer Geldbörse entwenden oder einen Online-Handelsplatz kompromittieren kann.

Die Diskussionen über kryptografische Währungen sind ein kleiner Teil der Diskussionen rund um Blockchains und deren mögliche Auswirkungen auf Staat, Wirtschaft und Gesellschaft. Spezifische Aspekte sind eher rechtlicher als technischer Natur und betreffen z. B. die grundsätzliche Frage, ob es sich überhaupt um eine Währung handelt, oder auch die Frage nach der Eignung als gesetzliches Zahlungsmittel und dem Umfang der staatlichen Regulierung.

Bewertung

Kryptografische Währungen könnten auf zweierlei Art im öffentlichen Bereich Einzug halten. Das ist zum einen durch die Akzeptanz von Kryptogeld zur Zahlung von Gebühren möglich. Die Schweizer Stadt Zug nimmt solche Beträge bis zu einer Höhe von etwa 200 Euro auch in Bitcoin entgegen. Dabei wurden im ersten halben Jahr seit Eröffnung dieser Möglichkeit rund 40 Vorgänge abgewickelt. Ob sich dieses Bezahlverfahren in Zug oder auch anderenorts durchsetzen kann, wird im Wesentlichen von der rechtlichen Stellung der Kryptowährungen im allgemeinen Finanzwesen abhängen.

Unabhängig von diesem Aspekt wird zum anderen auch diskutiert, ob öffentliche Verwaltungen selber werthaltige Transaktionen intern über kryptografische Methoden abwickeln können. Ob dabei eine eigene Währung entstünde oder in welchem Maße andere Aspekte der Blockchain-Technologie zum Tragen kämen, ist noch vollkommen offen. Es wird jedoch erwartet, dass ein solches Modell nicht gänzlich auf zentrale Steuerung verzichten würde.

KRYPTOWÄHRUNG

Verwaltungsrelevanz:

■□□□

Umsetzungsgeschwindigkeit:

■■□□

Marktreife/Produktverfügbarkeit:

■■■■

01

SCHNELLER OHNE BUS – NEUE RECHNERARCHITEKTUREN

Der Bedarf an Rechenleistung wächst durch die zunehmende Digitalisierung der Welt. Dies gilt sowohl in Bezug auf die zu verarbeitende Menge der Daten als auch im Hinblick auf die Geschwindigkeit der Verarbeitung. In klassischen Rechnerarchitekturen werden die zu verarbeitenden Daten über sog Bus-Systeme zwischen dem Speicher und dem Rechenwerk (CPU) transportiert. Die zugehörigen Betriebssysteme sind i. d. R. darauf ausgelegt, diesen Transport zu optimieren. Aber selbst bei kompakter Bauweise kosten die Wege im Computer Zeit und schon innerhalb der Prozessoren führt der Transport der Daten zu kleinen Verzögerungen in der Bearbeitung. So verwundert es nicht, dass seit Jahren daran geforscht wird, wie sich der Transport und das Speichermanagement in Rechnern optimieren lassen.

// 1 Petabyte ist eine Billiarde Bytes. 1 PB = 1 000 000 000 000 000 B = 10^{15} Bytes = 1 000 Terabyte .

Durch die Entwicklung von CPUs mit mehreren Rechenkernen (engl. „multi core CPU") kann die Verarbeitung beschleunigt werden. Doch diese Parallelität erfordert eine Koordination der Zugriffe auf die Daten in den Zwischenspeichern (Cache) der Rechenkerne. Mit wachsender Zahl der Kerne erhöht sich die Komplexität dieser Aufgabe und so wurde vielfach an der Verbesserung der Cache-Kohärenz gearbeitet. Ein Ansatz besteht darin, die Verbindungen zwischen den verschiedenen Bereichen auf einem Chip neu zu gestalten. In einem solchen Chip-Netzwerk (engl. „Network on a Chip", NoC) tauschen nur benachbarte Bereiche Kohärenzinformationen untereinander aus.

Weitere Verbesserungsmöglichkeiten der NoCs bzgl. Geschwindigkeit und Energieeffizienz durch die Verwendung von Lichtleitern auf den Chips an Stelle von elektrischen Leitern werden ebenfalls erforscht.

Einen noch radikaleren Ansatz wählte ein großer Computerhersteller und Technologiekonzern, der durch die Verwendung neuartiger Speicherbausteine, sog. Memristoren, die Trennung zwischen Dauer- und Rechenspeicher aufheben will. Indem Daten und Rechenwerk näher zusammenrücken, sollen viele Datentransporte im Rechner entfallen.

Auch bei dieser Architektur sollen Lichtleiter herkömmliche Leiterbahnen ersetzen und so den Zugriff auf Informationen im bis zu 160 Petabyte großen Speicher innerhalb von 250 Nanosekunden erlauben. Neben den Hardware-Neuerungen wird auch ein neuartiges, darauf abgestimmtes Betriebssystem benötigt, um die Vorteile der schnellen Technik nutzen zu können.

Doch noch lassen sich Memristoren nicht in großer Stückzahl produzieren, sodass der neue schnelle Superrechner erst einmal noch nicht realisierbar ist. Die neue Architektur, die den Speicher in den Mittelpunkt stellt, soll jedoch unter dem Namen „memory-driven computer architecture" auf der Basis existierender Hard- und Software weiter entwickelt und nutzbar gemacht werden.

Bewertung

Von schnelleren Rechnern, die bei weniger Platzbedarf noch bessere Energieeffizienz bieten, kann jede Branche profitieren, in der die Digitalisierung eine Rolle spielt. Dies gilt auch für die öffentliche Verwaltung.

Das Beispiel macht aber deutlich, dass disruptive Veränderungen schwierig sind, wenn Teiltechniken noch in der Entwicklung stecken. Erst wenn die Technik insgesamt das erwartete Potenzial ausschöpfen kann, sind große Verbesserungen im Anwendungsbereich – z. B. in Fachverfahren – möglich. Doch dazu bedarf es weiterhin der Grundlagenforschung, die ggf. in kleinen Schritten bereits zu Verbesserungen führt.

NEUE RECHNER-ARCHITEKTUREN

Verwaltungsrelevanz:

■□□□

Umsetzungs-geschwindigkeit:

■■■□

Marktreife/Produkt-verfügbarkeit:

■□□□

ANGEREICHERT, GEMISCHT, VIRTUELL – KRANK?

Freunde der Fernsehserien rund um die verschiedenen Enterprise-Raumschiffe kennen schon seit den 1980er-Jahren die Science-Fiction der sog. Holodecks. In diesen Räumen werden virtuelle Welten erzeugt, die nicht nur visuell und akustisch wahrgenommen werden können, sondern in denen künstliche Objekte auch haptisch – also mit dem Tastsinn – empfunden werden können.

In der Gegenwart sehen virtuelle Welten deutlich einfacher aus. Das liegt nicht nur an der fehlenden virtuellen Materie. Auch die grafische Darstellung ist noch weit davon entfernt, als real empfundene Bilder erzeugen zu können. Die Bilder werden nämlich zumeist auf mehr oder weniger großen „Monitoren" angezeigt, die mit einem brillen- oder helmartigen Gebilde am Kopf getragen werden. Trotzdem – oder gerade deswegen – erlebt das Thema „virtuelle Realität", kurz „VR", derzeit einen Boom, denn mit der zunehmenden Mobilität von IT durch Tablet-Computer, smarte Telefone und Uhren oder auch Lesegeräte für elektronische Bücher hat die Display-Technik in den letzten Jahren große Fortschritte gemacht. Die Zeiten, in denen eine Bildauflösung von 1024 x 768 Pixeln auf großen Bildschirmen als „erweitert" (engl. „extended") galt, sind lange vorbei und moderne „high-end" Smartphones haben Bildauflösungen von 1920 x 1080 Pixeln oder mehr. So verwundert es nicht, dass es inzwischen einige VR-"Brillen" gibt, die im Wesentlichen optisch unterstützte Halterungen für Smartphones sind. Schließlich bringen diese nicht nur den Bildschirm sondern auch noch Rechentechnik und Anwendungen mit.

Virtuelle Realität ist aber mehr als die Erzeugung hochqualitativer Bilder künstlicher Welten, die beim Betrachter den Eindruck erwecken, an fernen Orten oder in fremden Welten zu stehen. So, wie man sich in der realen Welt bewegen und dort agieren kann, soll es auch in der virtuellen Welt möglich sein. Eine wesentliche Voraussetzung dafür ist, dass sich das Bild vor dem Betrachter verändert, wenn er den Kopf bewegt. Dazu muss die VR-Ausrüstung derartige Bewegungen erkennen können und dann das gezeigte Bild entsprechend anpassen. Die möglichen Bewegungen des Kopfes beschränken sich dabei nicht auf das Drehen und Neigen, wie es bei der Anwendung im Sitzen der Fall ist. Auch Bewegungen im Raum müssen erkannt werden, wenn der Benutzer im Stehen bzw. Gehen handeln kann. Und schließlich müssen Gesten der Hände und das Greifen oder Bedienen von virtuellen Gegenständen bzw. Maschinen optisch nachvollziehbar sein.

Im realen Leben ist der Mensch beim Erkennen von Bewegung nicht allein auf optische Eindrücke angewiesen. Die akustische Wahrnehmung oder der Gleichgewichtssinn spielen dabei wichtige Rollen. Während Geräusche in der virtuellen Welt über Kopfhörer vermittelt werden können, sind die Empfindungen von Gleichgewicht oder Druck bzw. Berührung nicht so leicht zu simulieren.

Das Zusammenspiel der verschiedenen Sinne funktioniert in der Realität nahezu verzögerungsfrei. Die Sinne sind so aufeinander eingespielt, dass die Signale, die eine bestimmte Aktion auslöst, gleichzeitig wahrgenommen werden und so einen Gesamteindruck vermitteln. Reflexe, die es z. B. ermöglichen, einen Punkt mit den Augen zu fixieren, während man den Kopf bewegt (sog. „vestibulo-okulärer Reflex"), müssen in der virtuellen Welt durch komplexe Berechnungen nachgebildet werden. Wenn diese zu lange dauern, entsteht ein zeitlicher Versatz zwischen der Aktion des Nutzers und der sichtbaren Reaktion in der virtuellen Welt (Latenzzeit). Die optischen und anderen sinnlichen Eindrücke werden nicht mehr gleichzeitig verarbeitet. In beschränktem Umfang können derartige Störungen kompensiert werden – abhängig von der VR-Erfahrung des Anwenders. Nimmt die Verzögerung weiter zu, können die Störungen zu Übelkeit führen. Diese Simulatorkrankheit ähnelt der Reise- oder Seekrankheit. Verstärkt wird sie dadurch, dass der Körper versucht, optisch wahrgenommene

vermeintliche Bewegungen durch kleine Muskelbewegungen auszubalancieren und Veränderungen zu kompensieren, die tatsächlich nicht vorhanden sind.

// Die virtuelle Realität ist nicht der einzige Datenraum, in dem sich Anwender bewegen können. Während die VR aus gänzlich künstlich erzeugten Bildern besteht, wird bei der angereicherten oder erweiterten Realität die optische Wahrnehmung der realen Welt mit elektronischen Objekten überlagert.

Augmented Reality

Die virtuelle Realität ist nicht der einzige Datenraum, in dem sich Anwender bewegen können. Während die VR aus gänzlich künstlich erzeugten Bildern besteht, wird bei der sog. angereicherten oder erweiterten Realität (engl. „augmented reality", AR) die optische Wahrnehmung der realen Welt mit elektronischen Objekten überlagert. Diese werden entweder auf einem Monitor in das Bild der Umgebung eingeblendet oder auf einen transparenten Schirm projiziert, durch den der Anwender auf die reale Umgebung schaut. Dies kann zum Beispiel auch die Frontscheibe eines Autos oder Flugzeuges sein (sog. Head-up-Display). Bewegt sich jedoch der Anwender, muss auch hier das Gerät zur Dateneinblendung am Kopf getragen werden, um einen möglichst realistischen Eindruck zu erhalten. Die Synchronisation von physischer und erweiterter Realität gilt hierbei als noch kritischer als die latenzfreie Bewegung in der rein virtuellen Welt.

Auch für Smartphones und Tablets gibt es AR-Anwendungen. Diese Apps verknüpfen dann das von der Kamera aufgenommene Bild mit ihren Daten. So lassen sich z. B. die Namen von Berggipfeln ermitteln oder Flugzeuge am Himmel anhand ihrer Flugnummer identifizieren. Andere Apps beschränken sich auf die Auswertung des Standortes und der Geräteposition, um Sterne und Planeten am Himmel zu finden. Derlei Anwendungen verzichten jedoch oft auf den Versuch, Bewegungen latenzfrei umzusetzen, sodass dann in der Regel die Dateneinblendung nachjustiert wird.

Auch bei der Augmented Reality gibt es derzeit zahlreiche neue Entwicklungen. Mit der Jagd nach virtuellen Monstern in der realen Welt ist Augmented Reality zu einem Massenphänomen geworden. Ernsthaftere Anwendungen der Technik erlauben z. B. die Ergänzung von Produktpräsentationen oder die Unterstützung von Servicetechnikern jeweils durch die Markierung von Details, die Einblendung von Daten oder den Abruf von zusätzlichen Informationen. Die Interaktion mit der AR-Anwendung kann auf verschiedene Arten erfolgen. Bei Verwendung eines Touchscreens stellt dieser die Schnittstelle für Eingaben dar. Werden Brillen- oder Helmdisplays verwendet, erfordern Interaktionen zusätzliche Eingabegeräte – etwa ein Touchpad an der Display-Halterung oder ein separates Gerät, das im Raum bewegt und dabei bedient werden kann. Alternativ können auch Gesten zur Steuerung verwendet werden. Das bedarf aber zusätzlicher Sensoren im Raum, die die entsprechenden Bewegungen eindeutig erkennen. Dadurch ist die Mobilität der Anwendung jedoch sehr begrenzt.

Bei den AR-Systemen, die auf dem Kopf getragen werden, besteht derzeit eine weitere Einschränkung in dem geringen Blickwinkel, in dem virtuelle Objekte eingeblendet werden können. Das menschliche Auge erfasst optische Signale in einem Bereich von fast 180°. Und während einige VR-Systeme i. d. R. noch einen Winkel von rd. 100° darstellen, ist bei manchen modernen AR-Brillen der aktive Bereich auf 30° bis 40° beschränkt. Das führt dazu, dass virtuelle Objekte evtl. angeschnitten werden oder verschwinden, wenn man den Kopf

dreht. Trotzdem fallen aktuelle Erfahrungsberichte zu AR-Systemen oft positiv aus. Die gezeigten Objekte werden zumeist richtig im Raum platziert. Dies ist z. B. dann wichtig, wenn virtuelle Anwendungsfenster auf einer realen Wand dargestellt werden. Auch dreidimensionale Objekte, die man im realen Raum umrunden kann, können einen verblüffend realistischen Eindruck erwecken – sofern sie sich innerhalb des nutzbaren Winkels befinden.

Augmented Reality hat viele Anwendungsgebiete, auch wenn dabei derzeit eher experimentiert wird. Vielfach werden lediglich Zusatzinformationen zu wichtigen Objekten angezeigt. In kritischen Situationen kann die lagespezifische Orientierung im Gelände oder im Raum durch die zusätzliche Hervorhebung relevanter Objekte verbessert werden. Bei konstruktiven oder restaurativen Arbeiten können verborgene oder noch nicht realisierte Strukturen dem realen Bild überlagert werden. Dies kann in der Architektur, beim Bau oder auch in der Medizin die Arbeit unterstützen. Bei der Planung der Raumausstattung gibt es bereits entsprechende Anwendungen für Verbraucher. Erste Anwendungen, die als kommerzielle Standardprodukte die Echtzeitdiagnose von technischen Systemen oder virtuelles Training am Gerät unterstützen, unterstreichen die Ernsthaftigkeit derartiger Entwicklungen.

Durch die Vernetzung mehrerer Anwender sollen künftig gemeinsame Arbeit und gemeinsame Erlebnisse unterstützt werden. So verwundert es nicht, wenn ein soziales Netzwerk auch in diesem Feld aktiv ist. In den entsprechenden Szenarien verschwimmen ggf. die Grenzen zwischen der erweiterten und der rein virtuellen Realität, wenn sich Personen an verschiedenen Standorten befinden. Für einige kann zwar die reale Umgebung als „Hintergrundbild" für Augmentierung genutzt werden, für weiter entfernte Teilnehmer existiert diese Umgebung aber nur als Bild und damit als Teil ihrer virtuellen Realität.

Bewertung

Für die rein aktenbasierte öffentliche Verwaltung scheinen erweiterte oder gar virtuelle Realität zunächst keine Rolle zu spielen. Wenn in einem Fachverfahren alle relevanten Informationen elektronisch vorliegen und bearbeitet werden können, bringen optische Überblendungen von Informationen nur bedingt Zusatznutzen.

// Erweiterte und virtuelle Szenarien können auch in lageorientierten Anwendungsfällen bei der Beurteilung von spezifischen Situationen hilfreich sein.

Jedoch könnten erweiterte oder virtuelle Szenarien bei der Beurteilung von Vorgängen hilfreich sein. Dies betrifft zum einen lageorientierte Anwendungsfälle, in denen Informationen entsprechend der spezifischen Situation verfügbar gemacht werden. Zum anderen wäre es möglich, auch klassische Vorgänge zu unterstützen: Die zeitliche und räumliche Entwicklung von Bauvorhaben oder Naturschutzmaßnahmen oder auch die Auswirkungen sozial oder wirtschaftlich relevanter Projekte ließen sich so besser beurteilen. Hierbei dürften insbesondere Geodaten und georeferenzierte Daten der öffentlichen Verwaltungen eine Rolle spielen. Auch bei der retrospektiven Analyse von Ereignissen könnten Simulationen auf Basis erweiterter oder virtueller Realitäten die Arbeit oder auch Ausbildung von Spezialisten unterstützen. Bis dahin müssen AR und VR aber noch mindestens in zweierlei Hinsicht verbessert werden. Zum einen müssen Anwendungen mit angemessenem Aufwand realisierbar sein, die nicht nur einen Aha!-Effekt liefern, sondern die tägliche Arbeit erleichtern. Zum anderen müssen die gesundheitlichen Auswirkungen der Technik soweit verstanden und beherrscht werden, dass der praxisrelevante Einsatz möglich wird und nicht nur trainierten Spezialisten vorbehalten bleibt.

VIRTUELLE REALITÄT

Verwaltungsrelevanz:
■■□□

Umsetzungsgeschwindigkeit:
■□□□

Marktreife/Produktverfügbarkeit:
■■□□

01

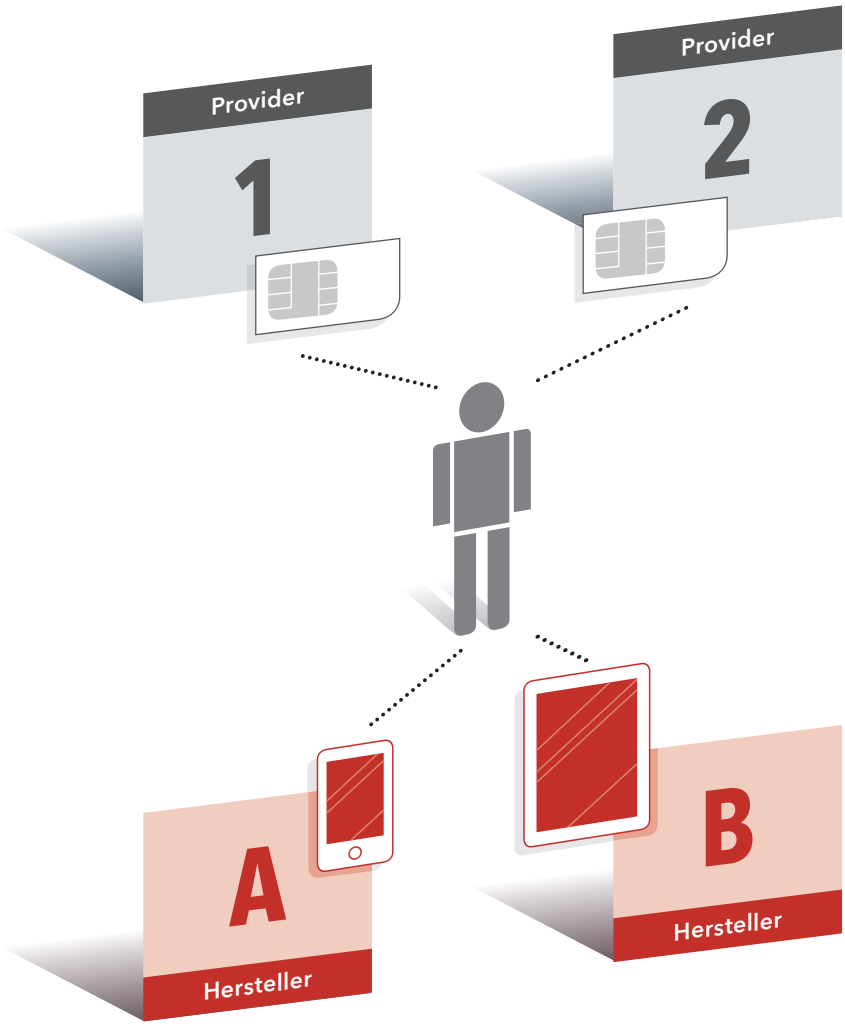
SIM-SALABIM – TRICKS MIT UND OHNE KARTE

Es gibt Dinge, die sind sehr wichtig, obwohl man sie so gut wie nie benutzt – z. B. eine Versicherung. Von der sieht man eigentlich nur dann etwas, wenn der Beitrag zu zahlen ist. Umso mehr ist man froh, sie zu haben, wenn man sie tatsächlich braucht. Andere Dinge, die wichtig sind, benutzt man ständig, ohne es zu merken. Wie abhängig man von ihnen ist, merkt man erst, wenn sie kaputt gehen oder aus anderem Grund gewechselt werden müssen. Ein Beispiel dafür ist die SIM-Karte, die – im Handy, Tablet oder einem anderen Gerät verborgen – ihren Dienst als „Teilnehmer-Identitätsmodul" (engl. „subscriber identity module", SIM) verrichtet. Die Karte taucht i. d. R. erst dann wieder auf, wenn man eine neue Telefonnummer bekommt oder den Telekommunikationsanbieter wechselt. Letzteres kann öfter vorkommen, wenn man häufiger auf Reisen im Ausland ist. Auch wenn die Roaming-Gebühren für die Nutzung von fremden Netzen zumindest in der EU begrenzt werden, ist es evtl. günstiger, für die Dauer der Reise einen am Ziel ansässigen Provider zu nutzen und dessen entsprechende SIM-Karte zu verwenden. Diese muss man dann entweder zusätzlich in sein Gerät einsetzen, oder – wenn das Gerät nur eine SIM-Karte aufnehmen kann – gegen die vorhandene Karte austauschen.

Die Möglichkeit, den Provider über einen Austausch der SIM-Karte wechseln zu können, zwingt die Hersteller von Handys, Tablets und anderen Geräten dazu, dem Nutzer den Zugang zu der Karte im Gerät zu ermöglichen und den Ein- und Ausbau einfach zu gestalten. Da die Karte über den zugehörigen Tarif einen gewissen Wert darstellt und über elektrische Anschlüsse verfügt, muss sie aber auch gegen Verlust respektive Feuchtigkeit geschützt werden. Daher werden die Karten i. d. R. in entsprechenden Haltevorrichtungen im Gehäuse untergebracht. Einigermaßen fest verankert sind sie dort gegen Spritzwasser geschützt. Trotzdem stellen die grundsätzlich zugänglichen Aufbewahrungsorte ein Problem dar, wenn ein Gerät wirklich wasserdicht gemacht werden soll. Das mag aus Sicht vieler Anwender ein Luxusproblem sein. Denkt man jedoch über Smartphone und Co. hinaus an das Internet der Dinge und welchen Bedingungen die mit Mobilfunktechnik vernetzten Objekte evtl. ausgesetzt sind, sieht das Bild schon ganz anders aus. Die sog. „Wearables" – insbesondere Fitness-Tracker oder smarte Kleidung – können bei verschiedenen Gelegenheiten nass werden, z. B. durch Schweiß, beim Duschen oder beim Waschen. Praktische Gründe sprechen also durchaus dafür, die SIM-Karte, die nichts anderes als ein gekapselter Chip ist, fest und geschützt im Gerät zu verbauen. Das hätte auch den Vorteil, dass der Platz für die Befestigungsmechanik der auswechselbaren Karten gespart werden könnte. Wäre da nicht das Problem der Providerauswahl...

Unter dem Stichwort „embedded SIM" (eSIM), also „eingebettete SIM", gibt es Bemühungen, eine fest integrierbare SIM-Karte zu etablieren. Die GSM Association, ein Verband von Mobilfunkanbietern, arbeitet an einem Standard für diese Technik. Neben der Spezifikation der üblichen Technik und ggf. des Formfaktors muss ein solcher Standard auch festlegen, wie der Umgang mit verschiedenen Providern gehandhabt werden soll. Die Grundidee besteht darin, die eSIM programmierbar zu machen. Dann kann ein Providerwechsel z. B. dadurch erfolgen, dass ein entsprechender Autorisationscode mit dem betroffenen Gerät eingescannt wird und die Daten des Mobilfunkvertrages auf der eSIM hinterlegt werden. Bei Geräten ohne Benutzeroberfläche kann eine solche Umstellung per Funk erfolgen. Um den kurzfristigen Wechsel von Provider oder Nummer zu vereinfachen, soll es möglich sein, die betreffenden Daten in Profilen abzulegen, die der Anwender dann bei Bedarf aktivieren kann. Und auch die Verwaltung mehrerer Geräte soll einfacher werden, wenn deren zugehörigen Profile eines Providers sich über einen Vertrag steuern lassen.

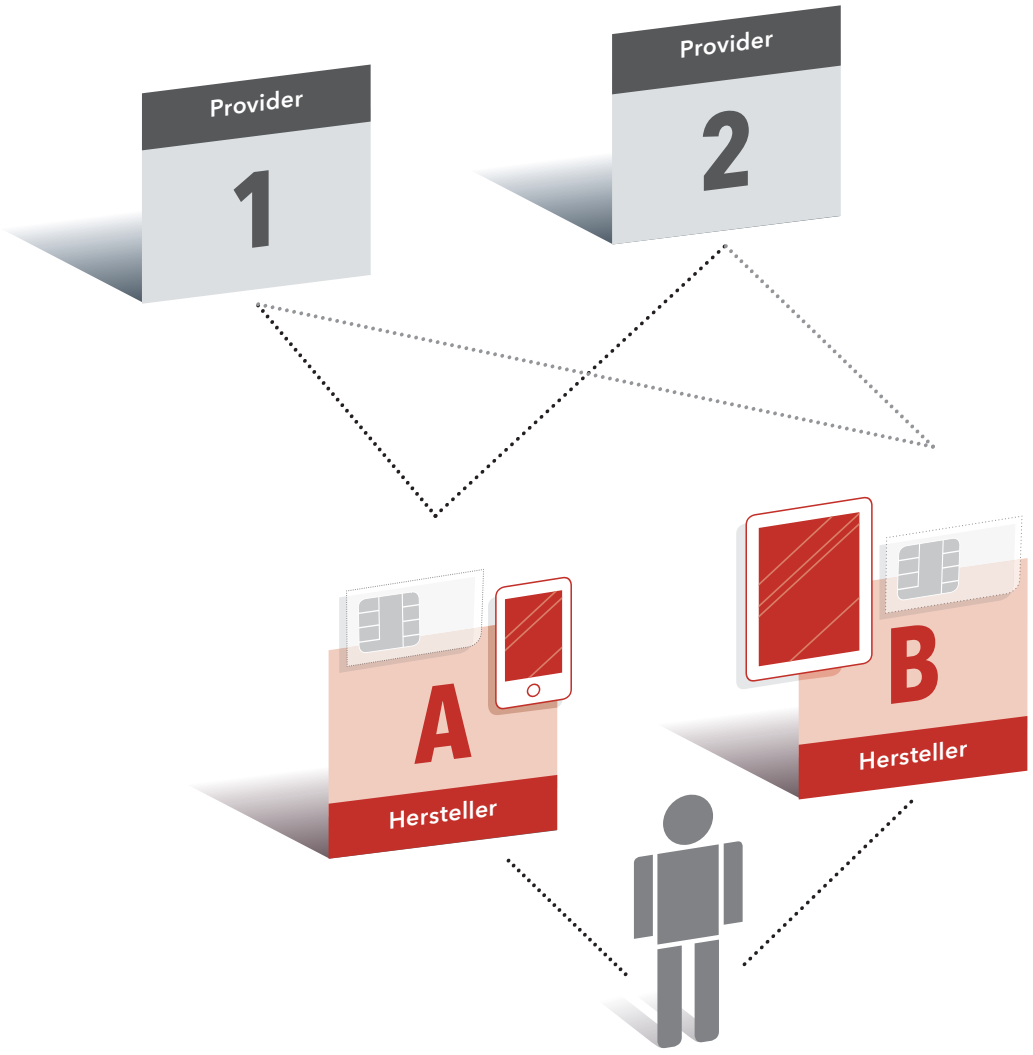
Eine besondere Situation stellt die erste Inbetriebnahme eines Gerätes mit einer eSIM dar, sofern dieses nicht im Verbund mit einem Mobilfunkvertrag gekauft wurde und ein Provider voreingestellt ist. Um die eSIM für den ersten Gebrauch einzurichten, muss ein Provider aus-



Bei der klassischen SIM-Karte kann der Anwender darüber entscheiden, welchen Provider er mit welchem Gerät nutzen möchte, und bei Bedarf Karten auswechseln.

gewählt werden. Dazu muss das Gerät eine Netzverbindung zu einem Profil-Dienst herstellen, der diese Auswahl ermöglicht. Ein System, das solche Dienste anbietet, wird Universal Discovery Server (UD-Server) genannt. Wer ihn betreiben soll, ist umstritten. Vieles spricht aber dafür, dass es eine unabhängige Stelle ist, die die verfügbaren Tarife und Profile für alle Provider gleichberechtigt behandelt. Das Erstellen der Profile könnte dagegen bei den (e)SIM-Kartenherstellern verbleiben, da diese bereits jetzt vergleichbare Aufgaben wahrnehmen. Die Auslieferung der Profile könnte durch Mobilfunkanbieter (engl. „Mobile Network Operator", MNO) oder Vermittler von Mobilfunkdiensten, die selber nicht über Netzinfrastruktur verfügen (engl. „Mobile Virtual Network Operator", MVNO), erfolgen.

Die Überlegungen zum UD-Server machen deutlich: An sich klingt das Konzept der eSIM sinnvoll und praktisch. Allerdings würden sich die Beziehungen zwischen den beteiligten Institutionen – um nicht zu sagen deren Abhängigkeiten untereinander – verändern. Beim Modell mit klassischen SIM-Karten hat der Anwender zwei voneinander unabhängige Verträge mit dem Mobilfunkanbieter bzw. mit dem Gerätehersteller. Dies gilt zumindest dann, wenn er nicht gezielt beide Leistungen im Paket von dem einen oder dem anderen Anbieter erwirbt. So kann er für sein Gerät recht einfach den Provider wechseln oder einen bestehenden Providervertrag mit einem anderen Gerät nutzen. Mit der eSIM kann die Abhängigkeit des Anwenders vom Gerätehersteller deut-



Bei der eSIM kann der Provider per Softwareanwendung eingestellt werden. Das ist flexibel, eröffnet dem Gerätehersteller aber Möglichkeiten, auf die Wahl des Providers Einfluss zu nehmen.

lich größer werden. Schon heute bestimmen die Macher der „Ökosysteme" von mobilen Plattformen darüber, welche Dienste, Inhalte und Leistungen dem Anwender zur Verfügung stehen. Indem den Anwendern die Möglichkeit genommen wird, den Provider per Kartentausch zu wechseln, gewinnt der „Herr über die Gerätesoftware" zusätzlich an Bedeutung.

Die Arbeiten an einer standardisierten eSIM sind noch nicht abgeschlossen. Zum Ende des Jahres 2016 war in Deutschland lediglich eine Smartwatch mit eSIM erhältlich. Schon seit einiger Zeit gibt es programmierbare SIM-Karten für den Einsatz in den Tabletcomputern eines bestimmten Herstellers, die jedoch nicht fest im Gerät verbaut werden. Die programmierbaren Funktionen sind hierbei noch auf einer Karte im normalen SIM-Format untergebracht, die dann wie üblich in das Gerät eingelegt wird. Über Einstellungen auf der Ebene des Betriebssystems kann dann der Provider ausgewählt werden. Jedoch ist eine Besonderheit in diesem System enthalten, die der Idee programmierbarer SIMs zuwider läuft. Die Profile der Provider können so gestaltet werden, dass sie die Karte an einen eingestellten Provider bindet. Dann ist ein Providerwechsel wieder nur möglich, wenn die Karte getauscht wird. Die Einsatzszenarien und das Zusammenspiel der

beteiligten Partner rund um die eSIM müssen sich noch entwickeln. Erste praktische Erfahrungen mit dem, was bei der eSIM sinnvoll und was möglich ist, müssen gesammelt werden. Sie können dann die geplanten technischen Rahmenbedingungen und die Geschäftsmodelle noch wesentlich verändern.

Bewertung

Für die Nutzer von Mobilfunktechniken gewinnt die Abwägung zwischen der flexiblen Handhabung von Providern und Tarifen einerseits und der Abhängigkeit von Lieferanten – insbesondere dem Gerätehersteller – andererseits mit der eSIM an Bedeutung. Für Organisationen mit vielen Mitarbeitern, deren Profile zur Nutzung von Mobilfunk sich nur wenig unterscheiden, dürfte sich in der Handhabung der Verträge nur wenig ändern, wenn der wesentliche Teil der Leistungen über Rahmenverträge beschafft wird. Allerdings kann auch gerade für sie der Wechsel der einen oder anderen Plattform – Mobilfunk oder Geräte – schwierig werden, wenn nur wenige und unterschiedliche Provider über die verschiedenen Systeme zur Verfügung stehen.

Eine Standardisierung der eSIM – nicht nur technisch sondern auch hinsichtlich der vertraglichen Regelungen und der Handhabung – dürfte ein wesentliches Erfolgskriterium sein. Spätestens wenn programmierbare SIMs ausschließlich fest verbaut in den Geräten und nicht mehr vom Anwender wechselbar sind, müssen geeignete kundenorientierte Modelle etabliert sein.

SIM-SALABIM MIT ESIM

Verwaltungsrelevanz:

Umsetzungsgeschwindigkeit:

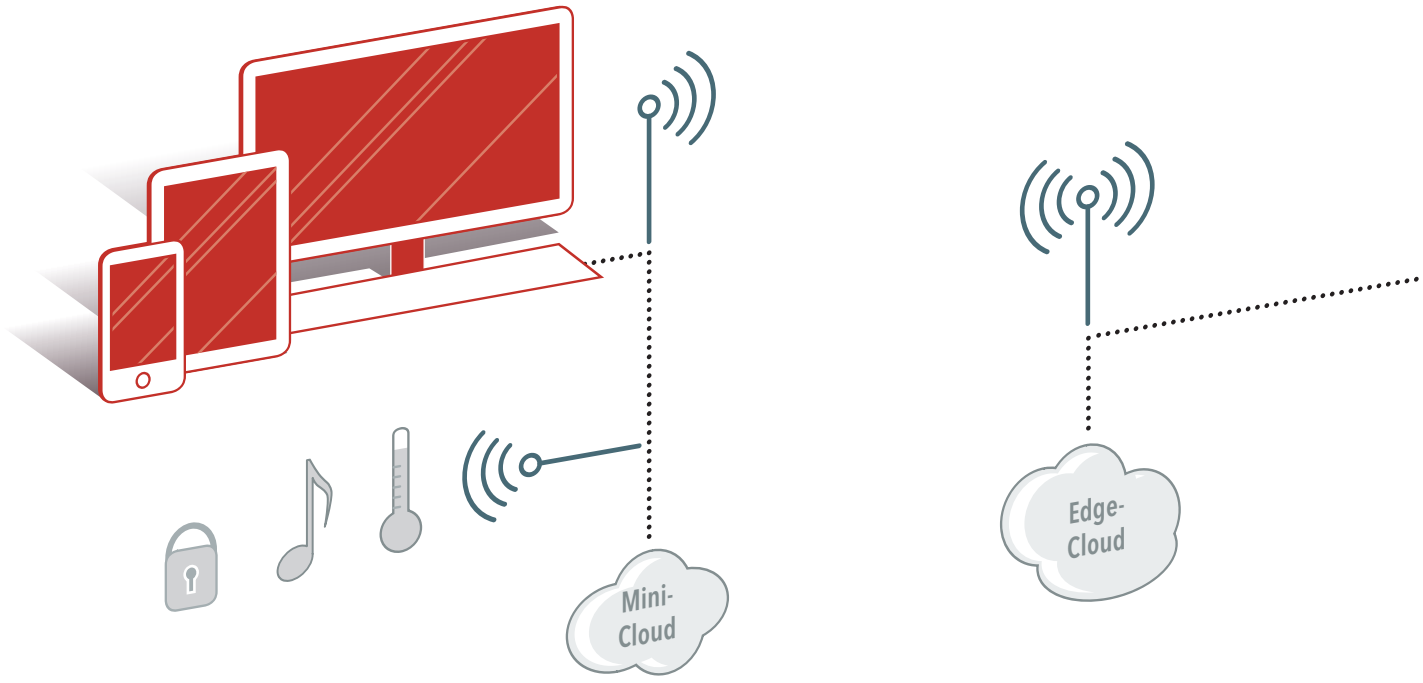
Marktreife/Produktverfügbarkeit:

INTERNET MIT VIEL GEFÜHL

Menschen und Tiere nehmen ihre Umwelt mit Hilfe zahlreicher Sensoren wahr. Einige Sinne wie Gehör-, Geschmacks-, Gesichts- oder Tastsinn benutzen wir täglich bewusst. Andere arbeiten eher im Hintergrund – etwa der Gleichgewichtssinn oder der Bewegungssinn (Kinästhesie). Verschiedene Tiere verfügen über weitere, stark ausgeprägte Sinne, die z. B. der Wahrnehmung elektrischer Felder (bei Haien) oder magnetischer Felder (bei Vögeln) dienen. All diese Sensoren stellen – technisch gesprochen – eine Schnittstelle des Lebewesens zu seiner Umwelt dar, die es ihm erlaubt, sich dort zurechtzufinden und angemessen zu agieren bzw. zu reagieren.

Auch technische Systeme werden zunehmend unter Berücksichtigung ihrer Umgebung betrieben. Sie arbeiten nicht mehr isoliert und nach einem starren Algorithmus, der für alle „Lebenslagen" gleich ist, sondern müssen vielmehr darauf reagieren, was um sie herum passiert. Ganz einfache Beispiele dafür sind Maschinen, die ihre Produktion drosseln bzw. stoppen, wenn der Speicher für ihre Arbeitsergebnisse voll ist oder der Nachschub von Rohmaterial ausbleibt. Ein Leerlauf der Maschine könnte diese beschädigen. Wo sich in der „Industrie 4.0" mehrere Maschinen oder gar Mensch und Maschine in die Quere kommen können, ist eine besondere Sensibilität erforderlich.

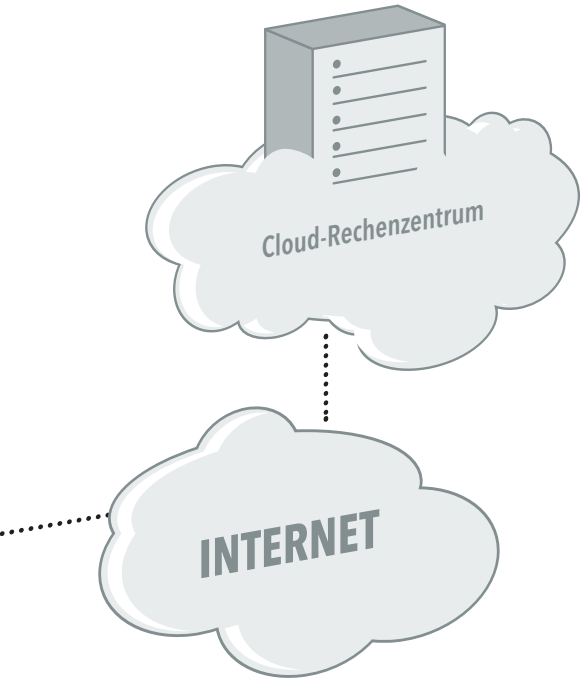
In der smarten Informationsgesellschaft haben elektronische Dienste, die auf die Umgebung reagieren, längst Einzug gehalten: Ortsabhängige Dienste (engl. „location based services") werden schon seit mehreren Jahren von intelligenten Anwendungen angeboten. Mit dem Internet der Dinge wird das Zusammenspiel von Umwelt, Technik und Mensch noch enger. Elektronische Sensoren übermitteln Informationen an die Anwender oder dienen sogar unmittelbar der Steuerung technischer Systeme – etwa bei der automatischen Bewässerung von Pflanzen. Das autonome Fahren von Autos ohne menschliches Zutun macht deutlich, welch komplexe Szenarien denkbar sind, und zeigt auf tragische Weise, was nicht ausreichende Sensorik bzw. falsche Interpretation von Daten für Folgen haben kann.



Die von Sensoren erfassten Daten werden möglichst lokal verarbeitet, da die Übertragung in entfernte Rechenzentren zeitkritisch sein kann.

Je mehr Informationen über die Umwelt erfasst werden, desto besser können sich Systeme und Anwendungen – und damit auch die Anwender – auf die jeweiligen Umstände einstellen. Mit der Erfassung allein ist es aber nicht getan. Die gesammelten Informationen müssen auch verarbeitet werden. Das setzt voraus, dass sie von den in der Umwelt verteilten Sensoren zu der entsprechenden Anwendung gelangen. Doch diese Übertragung von Daten benötigt Zeit. Beim Menschen liegt die Zeit, in der er – unbewusst – auf Reize reagiert, bei etwa einer Millisekunde. Das hat zur Folge, dass auch kleine Verzögerungen zwischen einem Signal und der entsprechenden Reaktion eines technischen Systems bei ihm zu Irritationen führen können. Der Prozess wird nicht als „natürlich" wahrgenommen (s. dazu auch Artikel „Angereichert, Gemischt, Virtuell – Krank?"). Gerade einen solchen natürlichen Umgang mit den vernetzten Objekten im Internet der Dinge zu ermöglichen, ist Ziel einer Reihe von Entwicklungen, die unter dem Namen „taktiles Internet" zusammengefasst werden. Dabei bedeutet „taktil", dass die Umwelt nicht aktiv abgetastet, sondern passiv wahrgenommen wird. Hier fallen evtl. große Mengen von Umweltdaten an. Um deren ausreichend schnelle Verarbeitung in „Echtzeit" zu gewährleisten, sind nicht nur schnelle Übertragungswege notwendig. Auch neue Hardware bis hin zum Chipdesign wird als notwendige Voraussetzung des taktilen Internets genannt.

Die schnellere Übertragung von Daten soll nicht allein auf höheren Datenraten beruhen. Auch wenn Funktechnik der fünften Generation (s. Artikel „2-, 3-, 4-, 5G-Qualität²") immer näher an die Geschwindigkeit von Leitungsnetzen heranreicht, garantiert das keine ausreichende Verarbeitungsgeschwindigkeit. So können z. B. durch Störungen verloren gegangene Datenpakete zwar erneut gesendet werden. Im Sinne des taktilen Internets würde dies aber eine deutlich spürbare Verzögerung zur Folge haben. Stattdessen wird z. B. untersucht, wie die



parallele Übertragung von Daten über mehrere Sender die nötigen Reaktionszeiten ermöglichen kann. Doch auch wenn die Daten sicher und mit hoher Geschwindigkeit fließen, hat ein weiterer Faktor Einfluss auf die sog. Latenz, also die Zeit zwischen dem Absenden und dem Empfangen der Daten, nämlich die Entfernung zwischen Sender und Empfänger. Das Internet der Dinge und die Verarbeitung großer Datenmengen in Cloud-Umgebungen werden oft in einem Atemzug genannt. Bei taktilen Anwendungen kann der Transport von Daten über längere Strecken vom Sender in ein evtl. weit entferntes Cloud-Rechenzentrum und von dort zurück zum Anwender selbst in Gigabit-Netzen zeitkritisch werden. Deshalb soll in den Fällen, bei denen lediglich lokale bzw. regionale Daten aus dem taktilen Internet verwendet werden, deren Verarbeitung dezentral erfolgen. Lokale Mini-Clouds und am Rande der Funknetze bei den Sendemasten bereitgestellte Edge-Clouds sollen die schnelle und bedarfsgerechte Verarbeitung der Daten in der Nähe des Geschehens ermöglichen. Dabei kann die verteilte Rechenleistung nicht immer mit umfangreicher Technik in beliebiger Größe realisiert werden. Hier spielen Hardware- und Chipdesigns eine Rolle, die sehr hohe Packungsdichten erlauben.

Die Herausforderungen des taktilen Internets sind nicht mit „ein bisschen mehr" bestehender oder etwas verbesserter Technik zu meistern. Neue Hard- und Softwarelösungen sowie Systemarchitekturen müssen dafür entwickelt werden. Wenn das taktile Internet als das wichtigste Infrastrukturprojekt des Jahrzehnts bezeichnet wird, unterstreicht das nicht nur seine mutmaßliche Bedeutung, sondern lässt auch erwarten, dass eine in der Informationstechnik vergleichsweise lange Zeit vergehen wird, bevor es Realität werden kann.

Bewertung

Verwaltungsabläufe, die durch ein taktiles Internet unmittelbar verändert werden, sind schwer vorstellbar. Mögliche Auswirkungen haben aber größere Datenmengen, die im Rahmen von Fachverfahren erfasst werden müssen und die die „äußeren Umstände" der Datenerhebung dokumentieren. Die Berücksichtigung dieser Umstände im Rahmen von Fachverfahren – z. B. bei der Bewertung von Sachverhalten – könnte dann mittelbar Einfluss auf Vorgänge haben. Neben den möglichen fachlichen Auswirkungen könnte das taktile Internet aber auch Einfluss auf die technische Infrastruktur von Verwaltungen haben. Die Netztopologie und die Verteilung von Anwendungen müssen ggf. an neue Anforderungen angepasst werden, wenn dezentral erfasste (Massen-)Daten eine Rolle spielen. Doch diese Veränderung wird nicht kurzfristig eintreten, wie die Einschätzung der Protagonisten deutlich macht.

Technologien wie das taktile Internet können nicht nur durch deren Anwendungen das Verwaltungshandeln beeinflussen. Wenn sie mehr und mehr in das tägliche Leben eingreifen, entsteht zusätzlicher Regelungsbedarf. Dieser betrifft einmal grundlegende rechtliche Aspekte, kann sich aber auch auf einzelne Fachverfahren erstrecken, sodass ggf. Prozesse angepasst oder neu definiert werden müssen.

INTERNET MIT VIEL GEFÜHL

Verwaltungsrelevanz:

■□□□

Umsetzungs-geschwindigkeit:

■■■□

Marktreife/Produkt-verfügbarkeit:

■□□□

02

ENTWICKLUNG // TECHNIK // NETZE

02

ENERGIESPAREN MIT PASSIVEM WI-FI

Wenn in einem Raum viele Personen gleichzeitig reden, versteht man nicht mehr viel. Die einzelnen Worte gehen im Rauschen des allgemeinen Geplappers unter. Ähnlich verhält es sich beim Radio und anderen Funktechniken. Hat man mehrere Sender, dann müssen sich diese darauf einigen, wie sie ihre Informationen an die Empfänger bringen, ohne sich gegenseitig zu stören. Ein weit verbreiteter technischer Trick besteht darin, das Signal, das die Informationen enthält, einem anderen Signal mit einer festen Frequenz zu überlagern. Der Empfänger, der die Veränderungen des Trägersignals erkennt, ist dann in der Lage, die Informationen wieder zu decodieren. Verschiedene Informationsströme kann man dadurch trennen, dass man entweder Trägersignale mit verschiedenen Frequenzen benutzt oder die Art, wie die Überlagerung der Signale erfolgt, verändert. Die Überlagerung von Trägersignalen mit Informationssignalen nennt man Modulation. Sie kann auf verschiedene Weise erfolgen, z. B. durch Veränderung der Lautstärke des Trägersignals (Amplitudenmodulation), der Frequenz (Frequenzmodulation) oder der Phase (Phasenmodulation).

// Die mobile Nutzung von Funktechnik wird durch deren hohen Energiebedarf erschwert. Mit passivem Wi-Fi soll der Energieverbrauch von funkenden Geräten gegenüber herkömmlichem Wi-Fi um den Faktor 10.000 kleiner werden.

Modulation wird in vielen technischen Bereichen verwendet. Neben Radio und Fernsehen nutzen dies auch Fernbedienungen, Amateurfunk, kabellose Kopfhörer, Satellitennavigation (GPS) und auch Datentechniken wie Ethernet, Bluetooth oder WLAN. Gerade bei den Funktechniken für Daten fällt jedoch ein Aspekt auf, der deren mobile Nutzung erschwert: Sie benötigen viel Energie. Bei Smartphone oder Tablet kann man die entsprechenden Funkverbindungen abschalten, um Strom zu sparen. Bei autonomen Geräten, die ohne Nutzerinteraktion ihre Dienste versehen, entfällt diese Möglichkeit. Daher werden immer wieder neue Wege gesucht, um anderweitig Energie zu sparen.

Eine vielversprechende Möglichkeit, den Energieverbrauch von WLAN-Technik nach dem Wi-Fi-Standard zu senken, haben nun amerikanische Wissenschaftler entwickelt. Mit dem sog. „passiven Wi-Fi" soll der Energieverbrauch bei den funkenden Geräten gegenüber herkömmlicher Wi-Fi-Technik um den Faktor 10.000 kleiner werden. Gegenüber Bluetooth LE (Low Energy) wäre das noch ein Faktor von 1.000. Möglich wird dies dadurch, dass die Erzeugung der Trägersignale und die der Informationssignale getrennt werden. Die Trägersignale werden durch analoge Hochfrequenztechnik (engl. „radio frequency", RF) erzeugt, die relativ viel Energie benötigt. Die Codierung der Information und Modulation der Signale kann mit digitaler Technik erfolgen, die deutlich energieschonender ist. Wenn die RF-Technik in ein separates Gerät eingebaut wird, können die Geräte, die die Informationen erzeugen, von dieser Arbeit entlastet werden. Die „Informationsquellen" können sich dann auf die Nutzung der sparsamen Digitaltechnik beschränken.

Das RF-Gerät wird mit einer Stromquelle verbunden und sendet permanent das Trägersignal aus. Die Modulation übernehmen die Informationsquellen, indem sie entsprechend der Codierung das Trägersignal reflektieren oder absorbieren. Dieser Vorgang benötigt so wenig Energie, dass sie direkt aus dem Trägersignal entnommen werden kann. Da hier das Datensignal nicht aktiv von der Quelle erzeugt wird, haben die Entwickler die Technik „passives Wi-Fi" genannt.

Dass dieser Ansatz sich mit dem Wi-Fi-Standard realisieren lässt, hat den großen Vorteil, dass die passiven Geräte mit herkömmlichen WLAN-Geräten zusammenarbeiten können. So ist z. B. kein spezieller WLAN-Router erforderlich. Die Entwickler erprobten die Technik mit allen Übertragungsraten, die der WLAN-Standard 802.11b

vorsieht. So ließen sich bis zu 11 MBit/s erreichen. Die Reichweite der Übertragung lag bei 10 bis 30 Metern. Die entwickelten Funkchips hatten dabei eine Leistungsaufnahme von 59,4 W.

Anwendungsfälle für das passive Wi-Fi finden sich insbesondere beim Internet der Dinge – auch in Szenarien, in denen vernetze Dinge nicht mobil sind. So könnten z. B. Steuerungen und Verbrauchmessungen im „Smart Home" oder in der Produktion einfach eingebunden werden, ohne sie mit überflüssiger Funktechnik „aufzublasen". Durch die Beschränkung auf das Notwendigste könnten die Dinge kompakter gebaut und kostengünstiger produziert werden. Doch ein wenig müssen wir uns noch gedulden, bis derart ausgestattete Geräte zu kaufen sind. Es wird erwartet, dass das passive Wi-Fi in zwei bis drei Jahren die Marktreife erreicht.

Bewertung

Es dürfte wenige spezifische Verwaltungsvorgänge geben, die auf WLAN-Technik überhaupt angewiesen sind. Insofern ist passives Wi-Fi unmittelbar wenig verwaltungsrelevant. Jedoch dürfte es das Internet der Dinge ein großes Stück weiterbringen, wenn die Energieversorgung der vernetzten Objekte weniger kritisch ist. So kann indirekt auch die öffentliche Verwaltung z. B. bei der Kontrolle und Steuerung ihrer Liegenschaften von passivem Wi-Fi profitieren – z. B. indem Raumbedingungen wie Licht und Klima auf die tatsächliche Nutzung eingestellt werden. Auch die vereinfachte automatische Datenerhebung im Rahmen von Fachverfahren könnte Vorgänge beschleunigen, wenn Medienbrüche durch „selbstregistrierende" Waren und Güter die Arbeit erleichtern.

PASSIVES WIFI

Verwaltungsrelevanz:

■■□□

Umsetzungsgeschwindigkeit:

■■■■

Marktreife/Produktverfügbarkeit:

■■□□

KOMMUNIKATION „LIGHT" MIT MQTT

Ein geist- und wortreiches Gespräch kann erbaulich sein, aber auch anstrengend. Das gilt nicht nur bei der Kommunikation zwischen Menschen, sondern auch zwischen Maschinen. Bei diesen spiegelt sich die „Anstrengung" in dem Aufwand nieder, den man betreiben muss, um die Kommunikation aufrecht zu erhalten. Der entsteht bei dem durch Protokolle formalisierten Nachrichtenaustausch zum einen durch die Daten, die für die Steuerung der Kommunikationsströme notwendig sind. Sie werden i. d. R. in einem definierten Bereich der Nachricht, dem sog. Header (engl. „head" für Kopf), untergebracht. Die inhaltlich flexibleren Informationen – sog. Nutzdaten oder engl. „payload" – werden im Rumpf der Nachricht (engl. „body") untergebracht.

Kommunikationsaufwand entsteht zum anderen dann, wenn die Zustellung der Nachrichten durch technische Bedingungen erschwert wird. Wie bei einer schlechten Telefonverbindung müssen dann Gesprächsteile evtl. wiederholt werden, denn verpasste Sprachfetzen verfälschen evtl. den Inhalt. Und schließlich benötigt eine aufwändigere Kommunikation auch mehr Energie.

> // Kommunikationsaufwand entsteht zum Beispiel dann, wenn die Zustellung der Nachrichten durch technische Bedingungen erschwert wird.

Wechselnde technische Rahmenbedingungen und der benötigte Energiebedarf sind beim Internet der Dinge zwei wichtige Themen – insbesondere dann, wenn die vernetzten Dinge mobil sind. Daher sind gerade hier leichtgewichtige Protokolle gefragt, bei denen der formale Teil der Kommunikation möglichst gering ist.

Für die Maschine-zu-Maschine-Kommunikation wurde mit MQTT (abkürzend für „Message Queue Telemetry Transport") ein leichtgewichtiges Protokoll entwickelt, das die Kommunika-

tion mit Sensoren und ähnlichen Dingen einfach und sicher machen soll. Es arbeitet oberhalb der Transportebene (OSI-Layer 4) und unterscheidet zwischen TCP/IP-basierten und anderen Netzen. Die Spezifikation nennt als Anwendungsgebiete beispielhaft Umgebungen, in denen eine Netzanbindung teuer oder unzuverlässig ist bzw. nur über eine geringe Bandbreite verfügt. Dazu kommen Szenarien mit eingebetteten Systemen, die nur über sehr beschränkte Rechen- oder Speicherkapazität verfügen.

Das MQTT zugrundeliegende Kommunikationsschema ist ein sog. publish/subscribe pattern. In einem solchen Modell werden Nachrichten von einem Kommunikationsteilnehmer veröffentlicht (engl. „publish") und von anderen Teilnehmern zum Empfang abonniert (engl. „subscribe"). Das bedeutet, dass der Sender einer Nachricht nicht unbedingt wissen muss, wer diese empfangen möchte. Je nach Anwendungsfall muss auch umgekehrt ein Empfänger nicht notwendig wissen, wer die Nachricht geschickt hat. Neben diesem grundlegenden Kommunikationsschema bietet MQTT eine Trennung zwischen Transportinformationen und Nutzdaten, eine dreistufige Steuerung der Kommunikationsqualität (Quality of Service) sowie eine Minimierung des Kommunikationsoverheads.

// Die vernetzten Dinge kommunizieren in einem MQTT-Verbund nicht direkt miteinander. Sie sind alle Clients, die mit einem zentralen System, dem Hub, sternförmig verbunden sind.

Der formale Teil der Kommunikation erfolgt mit Hilfe eines zweigeteilten Headers. Der erste Teil hat eine feste Länge von gerade einmal zwei Bytes und enthält Informationen wie die Art der Nachricht, die Servicequalität oder Flags, die anzeigen, dass es sich um das Duplikat einer Nachricht oder eine „gelagerte" Nachricht handelt. Letzteres kann dann hilfreich sein, wenn zwischen einzelnen Nachrichten viel Zeit vergeht und neue Abonnenten in einer Sendepause erste Nachrichten bekommen sollen. Schließlich wird im festen Header auch angegeben, wie viele Bytes noch zu der Nachricht gehören. Diese können zum variablen Header oder zum Nachrichtenrumpf gehören. Im variablen Header werden z. B. die „Themen" der Nachricht angegeben, anhand derer die Abonnenten die für sie interessanten Nachrichten identifizieren.

MQTT kennt vierzehn Typen von Nachrichten z. B. zum Einrichten oder Lösen einer Kommunikationsbeziehung (CONNECT bzw. DISCONNECT), zum Abonnieren (SUBSCRIBE) oder Veröffentlichen (PUBLISH). Nachrichten werden ggf. quittiert (engl. „acknowledge"). Nutzdaten werden lediglich von drei Typen ausgeliefert: CONNECT, SUBSCRIBE und SUBACK.

Hub und Broker

Die vernetzten Dinge kommunizieren in einem MQTT-Verbund nicht direkt miteinander. Sie sind alle Clients, die von einem zentralen System bedient werden. Dieser Hub, der die Clients sternförmig verbindet, hat die Funktion eines Brokers, d. h. er nimmt die versandten Informationen auf und sendet sie an die Abonnenten der entsprechenden Themen weiter.

MQTT wird als Internetstandard durch die Organization for the Advancement of Structured Information Standards (OASIS) entwickelt. Die Ports für MQTT – 1883 für die einfache Kommunikation, 8883 für die SSL-gesicherte Kommunikation – wurden durch die Internet Assigned Numbers Authority (IANA) standardisiert.

Der Wunsch, den Kommunikationsaufwand gering zu halten, ist durch mobile IT und das Internet der Dinge weit verbreitet. So verwundert es nicht, dass es weitere Protokolle gibt, die mit dem Anspruch antreten, leichtgewichtig zu sein, – z. B. CoAP, das wir 2014 im Trendbericht vorgestellt hatten. Bei der Wahl eines solchen Protokolls kommt es auf das konkrete Kommunikationsszenario an – und auf die Sicht der Ex-

perten. Während die einen für den Transport von Sensordaten MQTT empfehlen, führen andere dies als typisches Einsatzgebiet von CoAP an. Der Unterschied liegt in der Art und Weise, wie die Kommunikation erfolgt: Werden die Daten zielgerichtet und zweckorientiert übermittelt, um bei einem bestimmten Empfänger – oder auch mehreren – ein spezifisches Verhalten auszulösen, gilt CoAP als das Mittel der Wahl. Sind die Nutzer einer Information unbekannt und entscheidet der Empfänger selber über Sinn und Zweck von empfangenen Daten, wird MQTT empfohlen.

Bewertung

Wenn man Prognosen über zukünftig vernetzte Objekte liest – z. B. 50 Milliarden Geräte bis 2020 – steht das Internet der Dinge noch ganz am Anfang. So ist zu erwarten, dass auch die Entwicklung leichtgewichtiger Kommunikation eher noch mehr Protokolle und Varianten hervorbringen wird, als dass es zu einer Konsolidierung kommt. Dabei wäre es zumindest wünschenswert, dass diese Diversifizierung entlang von fachlichen Kriterien und Kommunikationsmustern erfolgt und nicht auch noch anhand von Herstellervorlieben.

Auch wenn das Internet der Dinge bisher in der öffentlichen Verwaltung noch nicht allgegenwärtig ist, gewinnt die Maschine-zu-Maschine-Kommunikation an Bedeutung. Insofern werden auch hier leichtgewichtige Protokolle zunehmend Anwendung finden. Welche das dann sind, hängt von den fachlichen und technischen Rahmenbedingungen im Einzelfall ab. Im besten Fall ist es für den Anwender sowieso unerheblich, welches Protokoll verwendet wird, solange die Kosten für Qualität überschaubar bleiben.

MQTT

Verwaltungsrelevanz:

Umsetzungsgeschwindigkeit:

Marktreife/Produktverfügbarkeit:

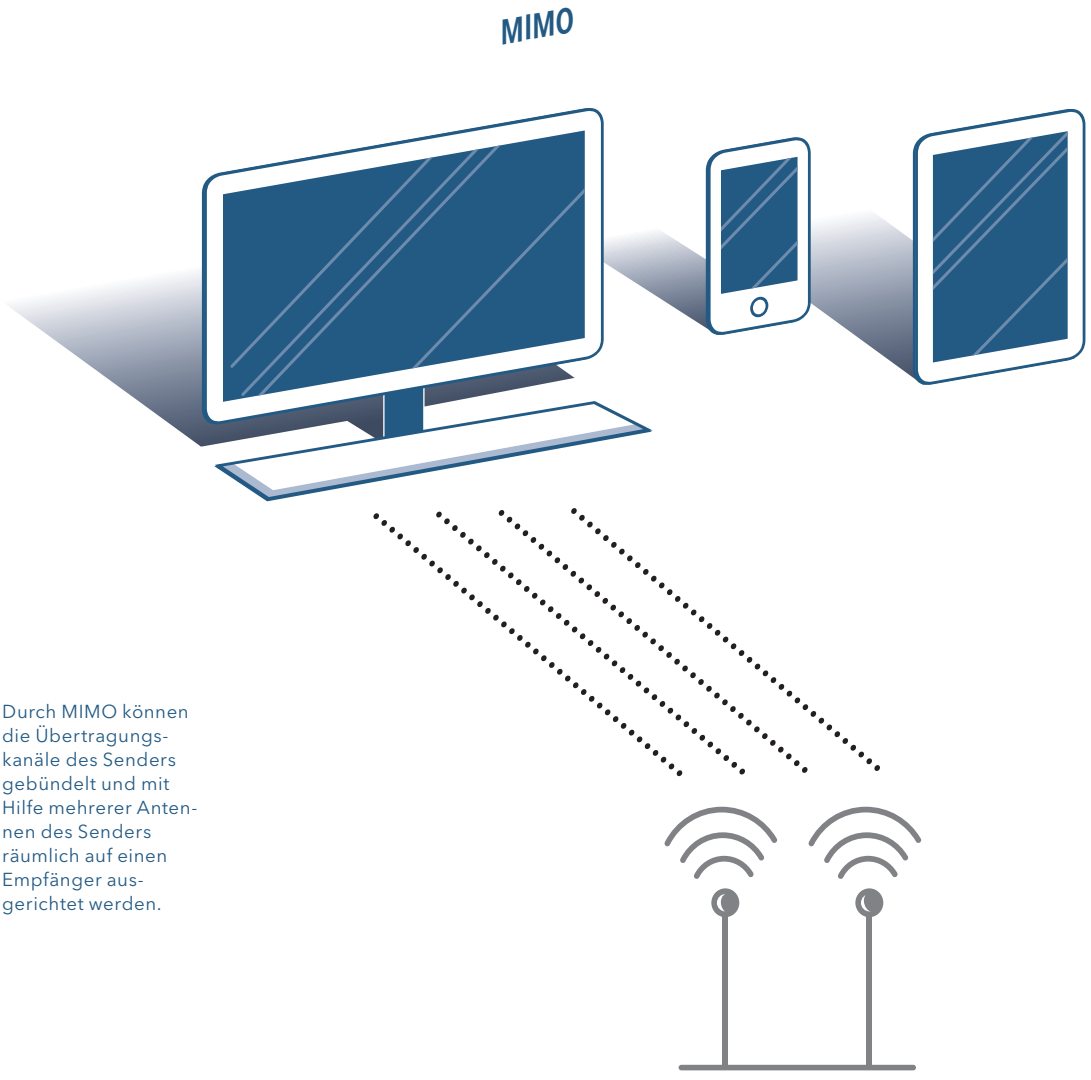
PARALLELGESPRÄCHE MIT MU-MIMO

In größeren Diskussionsrunden sind Parallelgespräche verpönt. Wenn mehrere Personen gleichzeitig reden, versteht kaum einer etwas. Darum schön der Reihe nach. Während einer redet, sind die anderen ruhig.

Was in Gruppen für geordnete Diskussionen sorgt, hat bei der elektronischen Kommunikation in Funknetzen zur Folge, dass viele Gesprächspartner einen wesentlichen Teil der Zeit nicht mit Daten versorgt werden können. I. d. R. kommuniziert ein Funksender mit einem einzelnen Empfänger, während die anderen Kanäle inaktiv sind. Da sich hier ein einzelner Empfänger – im Unterschied zu einer Diskussionsrunde – nicht dafür interessiert, was die anderen zu reden haben, führt dies zu viel Leerlauf. Wenn der Wechsel zwischen den angesprochenen Empfängern jedoch schnell genug erfolgt, entsteht für jeden Kommunikationskanal zumindest der Eindruck einer kontinuierlichen Datenversorgung – wenngleich nur mit einem Bruchteil der theoretisch zu erzielenden Datenrate des Senders. Damit ein Sender überhaupt mit mehreren Empfängern quasiparallel kommunizieren kann, wurde ein Verfahren entwickelt, bei dem Eingangs- und Ausgangsdatenströme über mehrere Antennen gesendet bzw. empfangen werden:

// Multiple Input Multiple Output (MIMO) dient dazu, die räumliche und zeitliche Verteilung von Funksignalen – und damit verschiedene Datenströme – von einem einzelnen Sender zu steuern.

Multiple Input Multiple Output (MIMO) organisiert dabei sowohl die zeitliche als auch die räumliche Verteilung der Signale. Dadurch lässt sich nicht nur die Abfolge der verschiedenen Datenströme steuern. Indem die Funkstrahlung

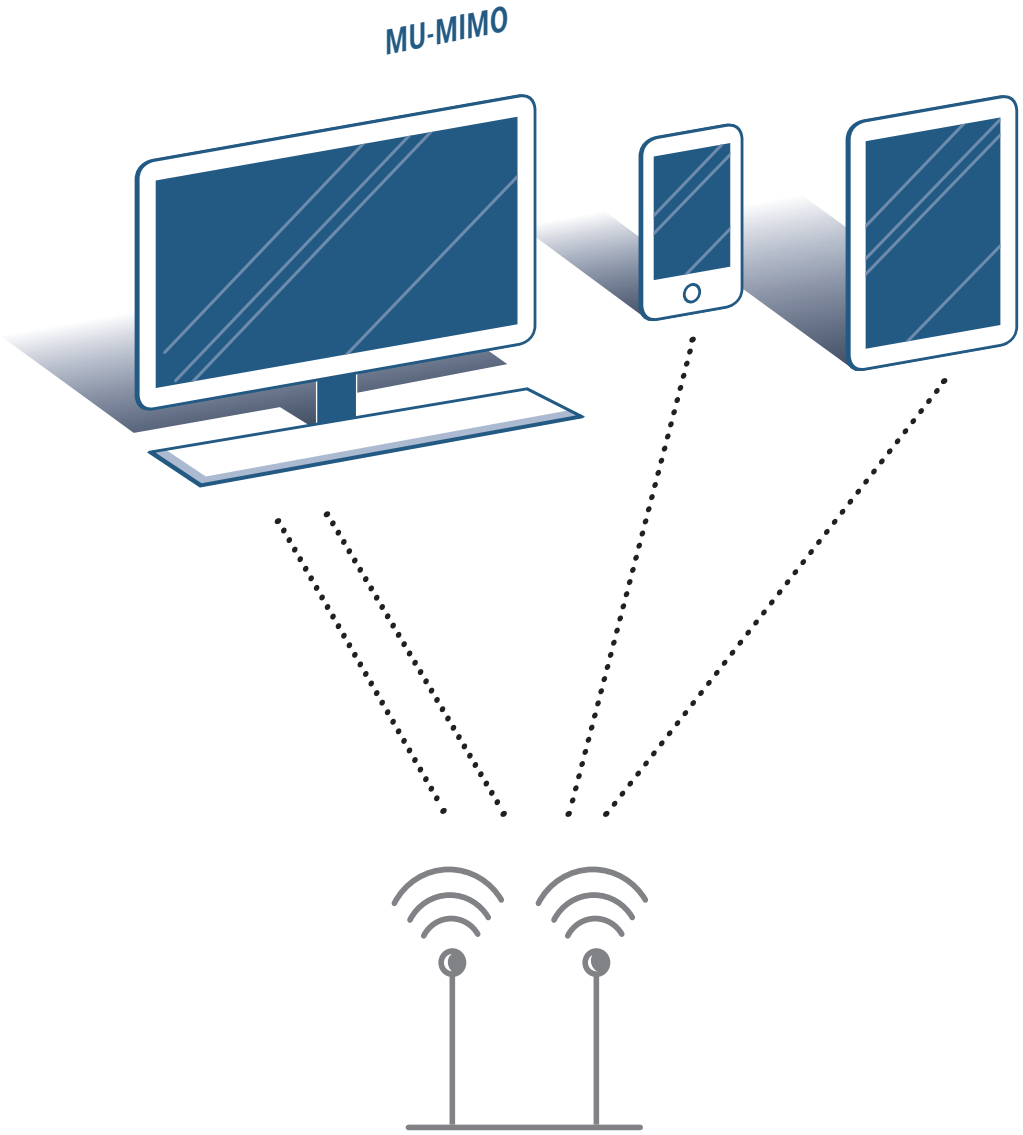


Durch MIMO können die Übertragungskanäle des Senders gebündelt und mit Hilfe mehrerer Antennen des Senders räumlich auf einen Empfänger ausgerichtet werden.

auf den jeweiligen Empfänger ausgerichtet wird, kann die Qualität der Übertragung verbessert werden. Durch das sog. Beamforming kann das Signal in der entsprechenden Richtung verstärkt werden, während es in den anderen Richtungen geschwächt wird.

Da beim klassischen MIMO zu jedem Zeitpunkt jeweils nur einer der Empfänger angesprochen wird, spricht man genauer auch von einem Einzelnutzer-MIMO, engl. Single User-MIMO (SU-MIMO).

Die Betonung dieser Tatsache weckt die Erwartung, dass es auch eine MIMO-Technik für die parallele Versorgung mehrerer Nutzer geben könnte. Und tatsächlich wurde mit dem Multi User-MIMO (MU-MIMO) eine solche entwickelt.



Bei MU-MIMO können die Übertragungskanäle des Senders mehrere Empfänger gleichzeitig versorgen.

Bei MU-MIMO können von einem Sender mehrere Empfänger gleichzeitig mit räumlich strukturierten Datenströmen (engl. spatial streams) versorgt werden. Für jeden Empfänger werden dabei wiederum mehrere Antennen verwendet. So kann jeder Datenstrom mit der bestmöglichen Übertragungsrate genutzt werden. Doch der Zugewinn an Geschwindigkeit hat seinen Preis. Dieser besteht weniger in einem Mehr an Antennenhardware, als vielmehr in dem Rechenaufwand für die Koordination der Antennen bzw. der Datenströme sowie für Anpassungen an sich ändernde Bedingungen: Wenn sich die räumliche Anordnung der Empfänger – z. B. von mobilen Endgeräten – ändert, muss die Ausrichtung der Signale angepasst werden. Dies erfordert eine ständige Kontrolle des Kanalzustandes und zusätzlichen Rechenaufwand im Sender. Daher

02

// Das MU-MIMO-Prinzip lässt sich mit verschiedenen Funktechniken anwenden. Derzeit wird es besonders zur Verbesserung der Netzversorgung in WLANs eingesetzt.

ist die Zahl der bedienbaren Empfänger i. d. R. auf vier begrenzt.

Das MU-MIMO-Prinzip lässt sich mit verschiedenen Funktechniken anwenden. Derzeit wird es besonders zur Verbesserung der Netzversorgung in WLANs eingesetzt (IEEE-Standard 802.11ac 2.0). Erste Router mit der Technik erscheinen auf dem Verbrauchermarkt. Da auch die Zielgeräte MU-MIMO beherrschen müssen, werden entsprechende Zusatzgeräte angeboten, die z. B. als USB-Stecker das Endgerät aufrüsten. Bereits 2014 waren durchschnittlich pro Haushalt in Deutschland 5,3 Geräte über WLAN vernetzt. Seither dürfte deren Zahl spürbar gestiegen sein. Und auch das über Netze konsumierte Datenvolumen – sei es aus dem Internet oder auch nur innerhalb des Hauses – ist z. B. infolge von Streaming-Diensten für Musik und Filme sicher nicht kleiner geworden. Da ist eine Verbesserung der Funkanbindung über WLAN willkommen.

MU-MIMO

Verwaltungsrelevanz:

■■□□

Umsetzungsgeschwindigkeit:

■■■□

Marktreife/Produktverfügbarkeit:

■■■□

Den Zuwachs an Übertragungsgeschwindigkeit bzw. Datenrate zu beziffern, ist schwierig. Zwischen den theoretisch zu erzielenden und den tatsächlich erreichten Werten klafft oft eine große Lücke – bedingt durch eine Vielzahl von Einflussgrößen, die zum Teil technikabhängig sind, zum Teil aber auch vom konkreten Einsatzszenario bestimmt werden. Zur Orientierung kann man sagen, dass Übertragungsraten oberhalb von 1 Gb/s mit den neuen WLAN-Funktechniken Normalität werden. Daraus ergibt sich aber eine neue Herausforderung, die vor allem in Heim- und anderen „kleinen" Netzwerken eine Rolle spielt: Wo die Netztechnik lediglich für 1 GB/s ausgelegt ist, wandert der Flaschenhals der Datenübertragung nun auf die kabelgebundene Seite des WLAN-Routers.

Neben MU-MIMO wird derzeit noch eine andere Verbesserung der MIMO-Technik entwickelt. Um sowohl die Geschwindigkeit als auch die Reichweite von Funknetzen mit MIMO-Technik zu erhöhen, wird bereits seit einiger Zeit an verteiltem MIMO (DMIMO für engl distributed MIMO) geforscht. Das Ziel dabei ist es, die Daten über die Sender in mehreren Geräten (Access Points) synchronisiert zu senden, sodass sich die Signale verstärken. Dabei besteht eine besondere Herausforderung darin, die automatische Verstärkungsregelung der einzelnen Sender aufeinander abzustimmen. Am Massachusetts Institute of Technology wurde nun unter dem Namen MegaMIMO eine Technik vorgestellt, die tatsächlich einen verteilten und synchronisierten Betrieb von mehreren Access-Points erlaubt und gegenüber herkömmlichem MIMO-WLAN eine Verbesserung der Sendeleistung um 260 Prozent erzielt.

Bewertung

Die Bereitstellung von Funknetzen ist derzeit in der öffentlichen Verwaltung wohl noch nicht der Normalfall. Doch auch hier gibt es Anwendungsszenarien, in denen insbesondere WLAN-Technik hilfreich ist – sei es in Konferenzräumen oder bei Arbeitsplätzen die nur sporadisch genutzt oder räumlich dynamisch gestaltet werden. Vor diesem Hintergrund dürften Funktechniken, die die gleichzeitige Versorgung mehrerer Geräte mit guter Leistung ermöglichen, auch hier zunehmend interessant werden. Damit Anwender tatsächlich von Techniken wie MU-MIMO profitieren können, müssen nicht nur entsprechende Access Points installiert, sondern deren Einsatz auch hinsichtlich der Anbindung, der Sendetechnik und der Clienttechnik geplant werden.

2-, 3-, 4-, 5G-QUALITÄT[2]?

Seit den ersten Tagen des mobilen Internets wird ständig versucht, sowohl die Leistung und Qualität der Informationsübermittlung als auch den Komfort der Nutzung zu verbessern. Jede der sog. Generationen brachte neue technische Merkmale und prägte neue Bezeichnungen für die jeweils aktuellen Standards: GPRS und EDGE in der 2. Generation (2G) oder UMTS, HSPA und LTE in der 3. Generation (3G). Dabei stellte LTE schon eine Weiterentwicklung dar, die unter der Generationsbezeichnung 3.9G den Übergang zur aktuellen 4. Generation (4G) mit LTE-Advanced kennzeichnete. Noch während die 4G-Technik weiter ausgerollt wird, arbeiten Mobilfunkausrüster und Netzanbieter bereits im Projekt „Next Generation Mobile Networks" an weiteren Verbesserungen für die 5. Generation (5G).

Allein die angestrebten Merkmale machen deutlich, dass sich die Mobilfunktechnik immer mehr der Leistung sehr schneller Leitungsnetze nähert. Neben Übertragungsraten von 10.000 MBit/s und Übertragungsverzögerungen (Latenzzeiten) von unter 1 ms stehen u. a. drastische Energieeinsparungen auf dem Plan. Doch diese und weitere Leistungsverbesserungen sind nur ein Aspekt der Entwicklung. 5G soll nicht nur Altbekanntes besser machen, sondern verfolgt auch eine neue Ausrichtung der mobilen Internettechnik. Im Fokus steht dabei die Verbesserung der Netzarchitektur, die den spezifischen Anforderungen verschiedener Dienste und Anwendungsszenarien entgegenkommt. So kommt es bei der Vernetzung von Geräten nicht unbedingt auf die schnelle Übertragung großer Datenvolumen, dafür aber ggf. auf nahezu verzögerungsfreie Kommunikation an (s. Artikel „Internet mit viel Gefühl"). Dagegen erhebt die Versorgung bewegter Objekte – etwa schneller Züge oder gar Flugzeuge – hohe Anforderungen an die räumliche Flexibilität einzelner Datenströme. Eine bemerkenswerte Eigenschaft ist die Möglichkeit, Geräte direkt miteinander zu verbinden, ohne dabei die Daten über ein Kernnetz transportieren zu müssen. So ist auch in permanent oder ereignisbedingt unversorgten Gebieten eine 5G-Kommunikation untereinander möglich.

Verschiedene Anwendungsszenarien sollen nicht mit jeweils spezifischer Hardware bedient werden, sondern in getrennten Netzabschnitten – sog. „slices" (engl. für „Scheibe"). Dazu sollen die möglichen Nutzerdienste als reproduzierbare Muster beschrieben werden. Je nach Anwendungsfall werden dann Instanzen dieser Dienste erzeugt (engl. „Service Instance"). Die für den Nutzerdienst benötigten Netzdienste werden in einer Instanz des Netzabschnitts (engl. „Network Slice Instance") umgesetzt. Dadurch wird auf Ebene der technischen und logischen Ressourcen eine Trennung der Dienste möglich.

> // 5G soll nicht nur Altbekanntes besser machen, sondern verfolgt auch eine neue Ausrichtung der mobilen Internettechnik. Im Fokus steht dabei die Verbesserung der Netzarchitektur für verschiedene Dienste und Anwendungsszenarien.

Network Slices werden ebenfalls als Instanzen aus Mustern (engl. „Blueprint") erzeugt. Eine solche Instanz kann mehrere Nutzerdienste der Anwendungsebene bedienen. Durch die Aufteilung der Netzressourcen, das sog. Slicing, können die spezifischen Anforderungen verschiedener Dienste parallel, aber getrennt voneinander umgesetzt werden. Das ermöglicht es, die jeweils benötigte Dienstgüte (engl. „Quality of Service", QoS) einzuhalten, ohne sie zu Lasten anderer Dienste temporär durch Priorisierung von Datenströmen zu erzwingen.

Derzeit werden die Spezifikationen für 5G noch entwickelt und erste Versuche durchgeführt. In Berlin wurde dafür ein Testfeld eingerichtet, das die Erprobung neuer Techniken außerhalb von Labors ermöglicht. Bis zum Jahr 2020 sollen 5G-Geräte am Markt verfügbar sein, bis 2025 soll das schnelle mobile Internet in den größten deutschen Städten und entlang aller wichtigen Transportstrecken verfügbar sein. Das setzt aber

2-, 3-, 4-, 5G-QUALITÄT²?

Verwaltungsrelevanz:

■■■□

Umsetzungs-geschwindigkeit:

■■■□

Marktreife/Produkt-verfügbarkeit:

■□□□

voraus, dass bis dahin auch die Infrastruktur bereitsteht, die den schnellen Transport der Daten von und zu den Funkzellen ermöglicht.

Bewertung

Nicht nur die Entwicklung der 5G-Technik ist noch im Gange, sondern auch die der Anwendungsfälle. In diesem Zusammenhang tauchen Fragen der Netzneutralität oder allgemeiner der Wechselwirkung verschiedenen Nutzerdienste auf. So muss z. B. geregelt werden, wie welche Dienste in Katastrophenfällen die Versorgung mit Daten und Kommunikation sicherstellen können.

Die höheren Leistungswerte von 5G kommen den Anwendern nur mittelbar zugute. Sie wirken sich weniger in der Wahrnehmung einzelner Dienste – z. B. eines Videostreams – aus, als vielmehr in der Verfügbarkeit eines breiten Dienste-Angebots.

Mit verbesserter Servicequalität – insbesondere hinsichtlich Geschwindigkeit und Verfügbarkeit – steigt die Attraktivität des mobilen Internets. Das hat nicht nur für Wirtschaft und Privatpersonen, sondern auch für die effiziente und effektive Verwaltung eine stärkere Abhängigkeit von der entsprechenden Technik zur Folge. Dies muss insbesondere in kritischen Anwendungsszenarien betrachtet und entsprechend abgesichert werden.

BLUETOOTH 5: HÖHER, SCHNELLER, WEITER – UND MEHR

Eigentlich könnte dieser Artikel sehr kurz ausfallen, denn die kommende Spezifikation des Funkstandards Bluetooth – dann in der Version 5 – scheint im Wesentlichen ein „Höher-Schneller-Weiter" im energiesparenden Modus vorzusehen: Die Übertragungsgeschwindigkeit der Daten soll sich gegenüber dem derzeitigen Standard (Version 4.2) verdoppeln und die Reichweite von bisher 50 m soll mit 200 m viermal so hoch liegen. Wie weit die Übertragung dann in der Praxis reichen wird, muss sich aber erst zeigen, denn oft lassen sich die berechneten oder unter Laborbedingungen erzielten Werte in der Praxis kaum erreichen. Dass es noch etwas mehr zur neuen Bluetooth-Version zu sagen gibt, liegt aber an einem weiteren Merkmal der Technik. Bluetooth ist nicht nur in der Lage, Daten in dezidierten Kommunikationsverbindungen mit einzelnen Geräten auszutauschen. Vielmehr kann ein Sender im sog. Broadcast-Modus auch Daten ausstrahlen, ohne zu wissen, welche Empfänger sie entgegennehmen – oder ob überhaupt jemand zuhört. Bisher können solche „Leuchtfeuer" (engl. „Beacon") Nachrichten mit einer Länge von lediglich 248 Bit, 31 sog. Oktetts (entsprechend je einem Byte), versenden. Das reicht i. d. R. gerade zur Identifikation des Senders und für einige wenige weitere Informationen. Aufgrund dieser Informationen sind dann Anwendungen – z. B. mobile Apps – in der Lage, zum Standort des Empfängers passende Informationen bereitzustellen. Der Umfang derartiger Nachrichten in den sog. Advertising Frames kann mit dem neuen Bluetooth 5 um das Achtfache erweitert werden. Mit dann 279 Oktetts lassen sich zwar keine Romane verbreiten. Der erweiterte Umfang entspricht aber immerhin zwei Botschaften des Kurznachrichtendienstes Twitter. Das bedeutet, dass z. B. Sensoren und andere vernetzte Dinge ihre Daten direkt allgemein zur Verfügung stellen können. Sie müssen nicht zunächst eine Verbindung zu einem Empfänger aufbauen, was vergleichsweise stromintensiv ist. Damit möchte die für die Bluetooth-Spezifikation zuständige Interessengruppe (SIG) den Standard insbesondere im Internet der Dinge gegen andere Techniken positionieren, etwa WLAN mit seiner neuen Vari-

// Beacons können künftig achtmal mehr Daten versenden.

ante „HaLow" oder das ursprünglich für schnurlose Telefone eingesetzte DECT mit dem energiesparenden ULE (kurz für „ultra low energy").

Bewertung

Wie bei jedem Trend, der im Kern einer Ausweitung des Leistungsspektrums entspricht, ist es schwierig, seine Bedeutung für die öffentliche Verwaltung abzuschätzen. Funktechniken für den Nahbereich dürften aber zunehmend Einfluss darauf haben, wie wir mit datenverarbeitender Technik umgehen, selbst wenn diese Verarbeitung in einzelnen Fällen unbemerkt geschieht.

Das kann mittelbar auch Verwaltungsabläufe verändern. Welchen Einfluss dabei aber eben Funktechniken wie Bluetooth haben, dürfte schwer festzustellen sein. Jedoch wird jeder, der via Bluetooth vernetzte Geräte verwendet, dankbar sein, wenn deren Einsatz weniger räumlich begrenzt sein wird – und trotzdem die Batterien länger halten.

BLUETOOTH 5.0

Verwaltungsrelevanz:

■□□□

Umsetzungsgeschwindigkeit:

■■■■

Marktreife/Produktverfügbarkeit:

■■■□

03

DATEN // INFORMATIONEN // SOFTWARE

03

DATA SCIENCE – EIN ALTER HUT?

Die Welt entwickelt sich immer weiter. Arten von Tieren und Pflanzen kommen und gehen. Viele davon bleiben lange Zeit unentdeckt, obwohl man annehmen könnte, heute sei alles erforscht. Das kann daran liegen, dass sich manche Spezies nur wenig, wenn auch signifikant, von ihren Verwandten unterscheidet. Und da wir Menschen gerne Unbekanntes auf Bekanntes zurückführen, heißt es dann schnell: „Das ist doch ein ...“ oder „Das sieht aus wie ...“

Nicht nur Arten von Lebewesen oder andere Teile der Natur verändern sich langsam. Auch Arbeitsweisen und Methoden werden – mal mehr, mal weniger bewusst – an Veränderungen in ihrer Umgebung angepasst. Und während die einen das Anderssein in den Blick nehmen und einen neuen Namen suchen, betonen andere die Gemeinsamkeiten mit Althergebrachtem: „Das machen wir schon seit 15 Jahren so.“ Beispiele aus der IT dafür sind Themen wie hyperkonvergente Systeme (s. HZD-Trendbericht 2016) oder Tablets, die „auch nicht mehr können als ein PC“ ...

// Zur Data Science gehört auch die Suche nach Informationen, von denen man nicht weiß, ob sie in den Daten enthalten sind.

Im Zusammenhang mit der Analyse von Daten taucht immer häufiger ein Begriff auf, der einerseits etwas Neuartiges verheißt, andererseits aber nur ein weiterer Name für Altbekanntes zu sein scheint: Data Science – die „Daten-Wissenschaft“. Je nach Blickwinkel heißt es dann, das sei doch nichts anderes als Statistik mit ein bisschen Programmierung versehen. Oder – anders herum – sei das doch auch nur Anwendungsentwicklung für statistische Analysen. Oder es handele sich doch lediglich um einen neuen Begriff für Business Analytics, also die Analyse von Geschäftsdaten.

Eine scharfe Definition des Begriffs bzw. eine Abgrenzung der Data Science gegenüber anderen Formen der Datenanalyse scheint in der Tat schwierig, denn die Liste der Elemente und Methoden aus anderen Gebieten, die in der Data Science verwendet werden, ist lang. Dazu gehören z. B.:

- Statistik,
- maschinelles Lernen,
- Software- und Data-Engineering,
- künstliche Intelligenz oder
- Big-Data-Analysen.

Viele der dabei auftauchenden Schlagworte bezeichnen ihrerseits Mischtechniken, die sich gegenseitig verwenden – etwa Data Mining, Predictive Analytics oder Data Warehousing. Auch Mustererkennung und Datenvisualisierung spielen bei der Data Science eine Rolle.

Einen Hinweis darauf, was die Data Science von vielen anderen Ansätzen der Datenanalyse unterscheiden kann, liefert der zweite Teil des Namens: „Science“, also „Wissenschaft“. Dieser schließt einerseits umfassende, bestehende Erkenntnisse ein, nimmt aber auch den Hinzugewinn neuer Erkenntnisse ins Visier. So versuchen manche Autoren, den Begriff „Data Science“ vor allem dadurch von anderen Analyse-Begriffen abzugrenzen, dass sie die Suche nach neuen Erkenntnissen explizit einschließen: Die herkömmliche Datenanalyse sucht i. d. R. nach Informationen, von denen man weiß, dass sie in den Daten stecken – etwa: „Welcher Kunde hat welche Waren bestellt?“. Zur Data Science gehört auch die Suche nach Informationen, von denen man nicht weiß, ob sie in den Daten enthalten sind – etwa ganz offen: „Was wissen wir über unsere Kunden?“

Neben der Analyse, was ist, wird also die Frage nach dem gestellt, was wahrscheinlich – oder gar, was möglich – ist. Das erfordert zum einen die Fähigkeit, mit wenig strukturierten Daten umgehen zu können, was die Verbindung zu Big-Data-Analysen herstellt. Zum anderen wird Sachkenntnis über das untersuchte Fachgebiet vom Datenwissenschaftler erwartet, wie auch die Fähigkeit, neue Erkenntnisse fachgerecht darstellen und vermitteln zu können.

Anwendungsgebiete für Data Science finden sich fast überall: Neben der Untersuchung von Wirtschafts-, Geschäfts- oder Finanzdaten werden z. B. auch Anwendungen in Gesundheitswesen, Biologie, Sozialwissenschaften oder so spezifischen Gebieten wie der Sprachanalyse genannt.

Bewertung

Ob sich das Profil der Data Science weiter schärft und zu einem spezifischen Berufsbild des Data Scientists führt, ist derzeit nicht absehbar. Zumindest werden auch in Deutschland erste Studiengänge und entsprechende Weiterbildungen angeboten. Für die öffentliche Verwaltung scheint Data Science auf den ersten Blick kein Betätigungsfeld zu sein, denn hier stehen i. d. R. spezifische Daten aus einzelnen Vorgängen im Vordergrund. Doch auch hier finden sich Anwendungen der einschlägigen Methoden – z. B. Im Hinblick auf präventive Maßnahmen im Zusammenhang mit dem Kriminalitätslagebild. Und es gibt sicher viele weitergehende Fragen nach Sachverhalten, die nicht bereits in einzelnen Vorgängen explizit festgehalten sind und von denen man gar nicht weiß, ob man etwas darüber weiß. Derartiges Wissen zu extrahieren und für die Steuerung großer Programme zu nutzen, könnte Aufgabe der Data Science im Öffentlichen Bereich sein. Dabei sind jedoch Zweckbegrenzung bzw. Zweckbindung der analysierten Daten zu beachten.

DATA SCIENCE

Verwaltungsrelevanz:

Umsetzungsgeschwindigkeit:

Marktreife/Produktverfügbarkeit:

CONTENT-DELIVERY 3.0

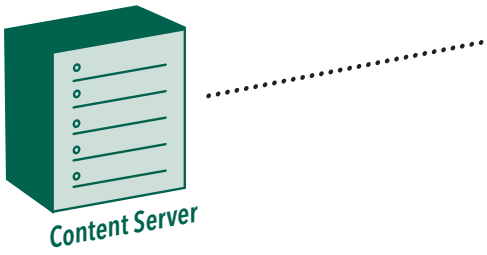
Der journalistische Inhalt von Publikationen ist eigentlich bedeutungslos. Er dient lediglich dazu, deren Zielgruppe so zu schärfen, dass die Werbung darin möglichst effektiv ist. – So könnte man denken, wenn man den aktuellen Wettstreit einiger großer IT-Unternehmen um die Vermarktung von journalistischen Beiträgen – dem sog. Content (engl. für Inhalt) – sieht. Maßgeschneiderte Werbung ist längst zu einem Motor des Internets geworden – oder besser zum Treibstoff, denn die von Suchmaschinen, sozialen Netzen oder anderen Ökosystemen damit erzielten Erlöse finanzieren immer mehr Projekte in der technisierten Welt. Die Währung, mit der der Treibstoff bezahlt und dieser werbefinanzierte Wirtschaftszweig am Laufen gehalten wird, ist schon lange nicht mehr der „Petrodollar" oder eine vergleichbare Größe des Finanzmarktes. Sie besteht vielmehr aus den Daten der Nutzer. Diese Daten werden, aufbereitet mit künstlicher Intelligenz und menschlicher Unterstützung, dazu genutzt, vorherzusagen, welche Werbung den potenziellen Leser eines inhaltlichen Beitrages verleiten könnte, den Weg zu einem anderen Angebot einzuschlagen und dort für realen Umsatz zu sorgen. Für Online-Publikationen – egal ob als eigenständiges Medium oder als digitale Ausgabe eines Druckwerks veröffentlicht – ist damit das Rezept für mehr Erlöse aus der Werbung relativ einfach: Im Kern muss die Reichweite der Beiträge, die mit Werbung garniert werden, erhöht werden: Je mehr Menschen den Beitrag lesen – oder zumindest sehen –, desto besser. Die Reichweite muss aber auch monetarisiert, sprich: „zu Geld gemacht" werden. Die Streitigkeiten zwischen Verlagen und Internetdiensten um die Frage, ob und wieviel Inhalt etwa in Suchmaschinen, Blogs oder sozialen Netzen kostenlos zitiert werden darf, drehen sich letztlich darum, auf welcher Plattform und damit von wem (Werbe-)Umsatz mit dem Content gemacht wird.

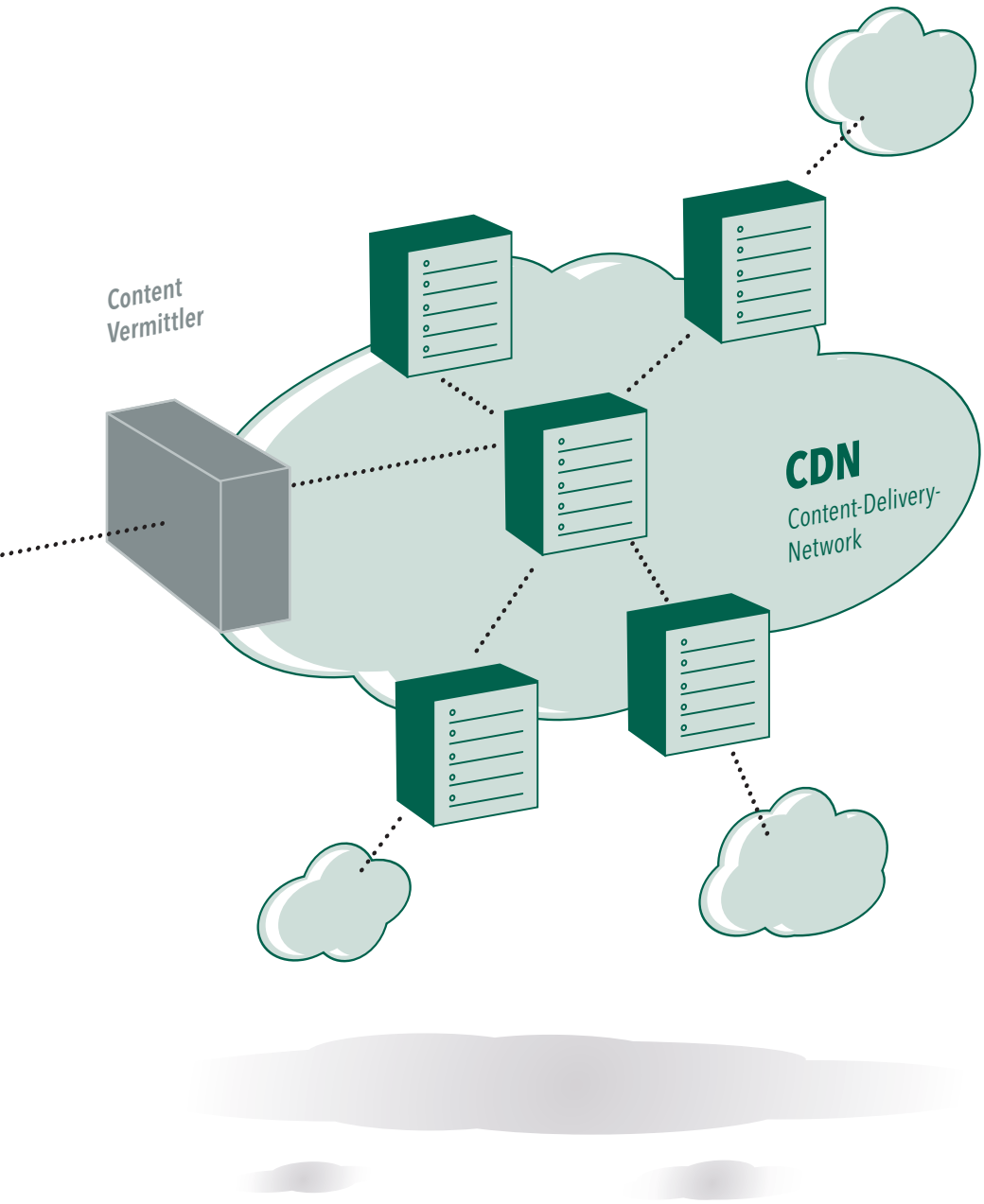
Neben den grundsätzlichen Überlegungen, wo das Geschäft mit dem Content gemacht wird, haben aber auch technische Aspekte Einfluss darauf, ob überhaupt Geschäft gemacht werden kann. Heutzutage sind schnelle Internetverbindungen für statischen Content weit verbreitet. Wenn nicht gerade große Datenmengen wie etwa beim Streaming von Musik oder Filmen über die Leitung geschoben werden, gehört der

quälend langsame Aufbau von Webseiten, bei denen man Element um Element einzeln erscheinen sieht, der Vergangenheit an. Oder wir sind in der mobilen Welt, denn Übertragungsengpässe in Funknetzen sind auch heute noch vielerorts an der Tagesordnung. Die Geschwindigkeit des Internets, die an der einen Stelle erlebt, aber kaum noch wahrgenommen wird, führt an der anderen Stelle dazu, dass bei langsamer Contentübertragung der Nutzer ungeduldig wird und den Vorgang abbricht, noch bevor die Seite – und damit die erlösbringende Werbung – angekommen ist. Die Aufbereitung von Webseiten für verschiedene technische Umgebungen und ihre Optimierung unter dem Gesichtspunkt der „Netzkosten", z. B. Übertragungsvolumen und -dauer, ist durchaus aufwändig. Hierbei geht es nicht allein um die Anpassung von Layout und Bedienelementen (Stichwort „responsive design"). Insbesondere bei einem Medienmix aus Texten, Audio- und Videoformaten müssen ggf. auch die einzelnen Inhalte optimiert werden. Und schließlich trägt die eingebettete Werbung, die i. d. R. von verschiedenen Anbietern kommt und die Inhaltsseite mit vielen fremden Webdiensten verbindet, erheblich zum langsamen Aufbau der Webseiten bei.

In dieser Situation scheint Hilfe von verschiedenen IT-Konzernen zu kommen, die technische Frameworks zur schnellen Auslieferung von mobilen Webseiten – einschließlich Werbung – entwickelt haben. Im Wesentlichen basieren diese Techniken auf HTML und JavaScript, ergänzt um einige spezifische Erweiterungen. Unterstützt werden die Techniken durch Werkzeuge für etablierte Content-Systeme, z. B. in Form von Plugins. Die Entwicklungen der Frameworks erfolgen entweder im Ökosystem der jeweiligen Firma – etwa als die sog. „Instant Articles" eines sozialen Netzwerks – oder, wie im Fall von „Accelerated Mobile Pages" (AMP) des Suchmaschinenanbieters, im Rahmen eines Open-Source-Projektes.

Die Aufbereitung des Contents bzw. der Webseiten ist aber nur ein Element der neuen Entwicklungen, durch die die mobilen Seiten beschleunigt werden sollen. Ein zweites Element ist die Verteiltechnik. Schon seit langem – im Trendbericht 2004 berichteten wir darüber – werden Netze zur schnellen und sicheren Auslieferung von Webinhalten gebaut. Diese sog. Content Delivery Networks (CDN) optimieren die Lastverteilung für die zentralen Komponenten und entlasten diese zusätzlich durch Zwischenspeicher (engl. „cache"), die die Daten z. B. für bestimmte Regionen zur Verfügung stellen. Doch so ein CDN kann komplex werden und da liegt es nahe, die Verteilung der Inhalte an einen Diensteanbieter auszulagern, der so-





Nutzt der Content-Anbieter die Dienste und die Infrastruktur eines Vermittlers, gibt es an ihn auch die Kontrolle darüber ab, welche Inhalte verteilt werden.

wieso schon über derartige Infrastrukturen verfügt. Wenn dieser Diensteanbieter dann auch noch ein wesentlicher „Lieferant" der Inhalte – und der Werbung – für die Leser ist, wie etwa eine Suchmaschine oder ein soziales Netzwerk, scheint die Partnerschaft perfekt. Doch ist zu bedenken, dass der Diensteanbieter zwar Leser und Inhalte zusammenbringt, dies aber nicht auf der Plattform des Content-Anbieters tut. Vielmehr erhält er von diesem die Inhalte und präsentiert sie dann seinen eigenen Nutzern. Dies trägt zur angestrebten Beschleunigung bei, da die Weiterleitung an einen anderen Server, nämlich den des Content-Anbieters, entfällt. Dieser Ansatz legt aber auch einen wesentlichen Teil der Kontrolle über die Inhalte in die Hände des vermittelnden Dienstes. Dass dies keine rein theoretische Überlegung ist, wird deutlich, wenn man das Prozedere anschaut, das die Herausgeber für Inhalte im Fall des o. g. sozialen Netzwerks durchlaufen: Die müssen sich nämlich mit 50 vorbereiteten Artikeln – einschließlich ge-

wünschter Werbeanzeigen – einer Prüfung durch den Betreiber des Netzwerks unterziehen, bei der festgestellt wird, ob der Herausgeber die dort gültigen Regularien für Inhalte und Werbung einhält.

Das Gesicht der Presse hat sich durch das allgegenwärtige Internet verändert und wird sich weiter verändern. Das ist keine neue Erkenntnis, wie auch die Feststellung, dass die elektronischen Medien Druckerzeugnisse immer mehr in die Ecke drängen und der Werbemarkt in das Internet abwandert. Die neuen Techniken zeigen aber auch, dass sich die Rolle der heutigen Medienproduzenten verändert. So wie ihnen die Nachrichtenagenturen die Kernmeldungen liefern, könnten sie selber künftig zu Lieferanten von aufbereiteten Inhalten degenerieren, während die Verteilung und Präsentation den Eigentümern der Infrastruktur überlassen wird. Schon heute bestimmen diese mit zahlreichen Regeln, was wie veröffentlicht werden darf – oder nicht. Mit der Konzentration der wesentlichen Content-Plattformen auf einige wenige Anbieter hängen Nachrichten und Informationen aller Art von deren Geschäftsinteressen und technologischen Vorlieben ab. So verwundert es nicht, wenn für den Bereich Content Delivery ähnlicher Regulierungsbedarf gesehen wird wie bei den Betreibern informationstechnischer Infrastrukturen.

CONTENT-DELIEVERY 3.0

Verwaltungsrelevanz:

■□□□

Umsetzungs-geschwindigkeit:

■■■□

Marktreife/Produkt-verfügbarkeit:

■■■■

Bewertung

Öffentliche Verwaltungen sind weder journalistisch tätig, noch finanzieren sie ihre Tätigkeiten durch Werbung. Trotzdem sind auch sie mit ihren Informationsangeboten Lieferanten für Webinhalte.

Das Anliegen und die Notwendigkeit, diese Informationen zu den Verwaltungskunden – Bürgerinnen und Bürgern wie auch Firmen und Organisationen – zu bringen, kann von den neuen Techniken profitieren. Insofern liegt es einerseits nahe, deren Einsatz bzw. Nutzung zu prüfen. Andererseits können die staatlichen Informationspflichten nicht ohne weiteres an wenige einzelne Dienstleister ausgelagert werden, die mit ihren Plattformen marktbeherrschend sind und damit festlegen, was wo und wie verbreitet wird.

PROGRAMMIEREN MIT STIL – UND VERWIRRUNG

Wenn man sagt, jemand habe Stil, kommt dadurch zum Ausdruck, dass die bewusste Person Dinge, die mehr oder weniger alltäglich sind, in einer besonderen Art und Weise tut. Das Ergebnis hat dann jeweils eine typische oder gar spezifische Erscheinungsform, die der Betrachter mit der Person verbindet. „Ein reinrassiger Picasso." – „Typisch Hemingway!" – „Unverkennbar Bach!" – so oder ähnlich lauten dann die Urteile, wenn man ein vom Stil geprägtes Werk betrachtet, liest resp. hört. Kenner und Experten können auch ihnen unbekannte Werke oft dem jeweiligen Erschaffer zuordnen. Dabei helfen das richtige Gefühl oder auch eine Reihe von immer wiederkehrenden Merkmalen im Œuvre der Meister. Die Zuordnung von Schriftstücken zu ihren Autoren anhand solcher Merkmale heißt Stilometrie. Der Begriff entstand bereits im 19. Jhd. Die Stilometrie analysiert Werke verschiedener Autoren, aus verschiedenen Genres oder Epochen und charakterisiert die einzelnen Stile mit Hilfe der Statistik.

Die Frage, wer etwas geschrieben hat, bewegt nicht erst seit dem unter dem Pseudonym Robert Galbraith geschriebenen Kriminalroman der Harry-Potter-Autorin oder im Zusammenhang mit verschiedenen Plagiatsaffären die Gemüter. Die Stilometrie ist auch Teil der forensi-

schen Linguistik, mit der Kriminalisten versuchen, Schriftstücke wie Erpresserbriefe oder Geständnisse ihren wahren Verfassern zuzuordnen. Interessante Stilmerkmale, die dabei untersucht werden, sind etwa Satzlänge, die Häufigkeit einzelner Wörter oder die Verwendung von Einzelwörtern, die Vielfalt des Wortschatzes oder auch syntaktische Eigenschaften der Texte.

Seit einiger Zeit werden stilometrische Methoden auch bei der Analyse von Software angewendet und weiter entwickelt. Hier kann die Autorenschaft eine wichtige Rolle spielen, etwa wenn es um Fragen des Urheberrechts geht. Auch bei der Suche nach den Verfassern von Schadsoftware kommt die Stilometrie zum Einsatz.

Programmiersprachen sind formale Sprachen mit einem i. d. R. sehr beschränkten Wortschatz. Trotzdem ist es auch mit ihnen möglich, einen individuellen Programmierstil zu entwickeln. Zu den Merkmalen, die diesen Stil beeinflussen, gehören solche, die den „Wortschatz" betreffen:

Lexikalische Merkmale wie

- Häufigkeit von Einzelwörtern,
- Häufigkeit von Schlüsselwörtern der Sprache (z. B. if, else, while),
- durchschnittliche Anzahl von Parametern bei Funktionen oder
- Schachtelungstiefe von Schleifen.

Auch die Gestaltung des Programms beeinflusst den Stil:

Layout-Merkmale wie

- Häufigkeit von Tabulator- oder Leerzeichen (z. B. Einrückungen),
- Häufigkeit von Leerzeilen oder
- Vorhandensein von Zeilenumbrüchen vor Codeblöcken, die in Klammern stehen.

Syntaktische Merkmale können anhand sog. „abstrakter Syntaxbäume" (AST für engl. „abstract syntax tree") einzelner Funktionen analysiert werden und umfassen dann Merkmale wie:

Syntaktische Merkmale

- Maximale Tiefe der AST,
- Häufigkeit bestimmter „Knotentypen" in den AST oder
- Häufigkeit von einzelnen Code-Elementen (Code-Unigramme) in den Blättern der AST.

Anhand derartiger Merkmale lassen sich verschiedene Programmierstile durchaus erkennen. Dabei hängt die Zuverlässigkeit der Prüfmethoden von verschiedenen Faktoren ab. Wichtig ist z. B. der Umfang der Vergleichs- bzw. Trainingsbasis, wenn stilometrische Verfahren lernen, Stile zu erkennen. Auch die Anzahl der in Frage kommenden Autoren hat einen Einfluss auf die Erfolgsquote. Für den Erfolg im praktischen Einsatz – z. B. in der Software-Forensik – ist natürlich wichtig, ob man davon ausgehen kann, dass der unbekannte Verfasser des analysierten Codes in der Vergleichsbasis vorhanden ist, oder nicht. Für die Suche nach den Autoren von Schadsoftware ist daher eine gute Datenbasis erforderlich. Diese muss nicht nur möglichst umfangreich sein, sondern auch die Vergleichbarkeit von Codeausschnitten erlauben. Ähnlich wie das Genre eines Textes den Stil von Literatur beeinflusst, hat auch die Aufgabenstellung auf den Stil der Programmierung Einfluss. Schwierige Aufgaben können zu einer stärkeren Differenzierung der Merkmale führen, da erfahrene Programmierer hier eher in der Lage sind, trickreichen Code zu schreiben, als weniger erfahrene. Eine gute Datenbasis ergibt sich aus Programmierwettbewerben, bei denen ggf. viele verschiedene Lösungen zu einer einzelnen spezifischen Aufgabe implementiert werden. Daher fördern technische Geheimdienste z. B. in

// Aus Programmierwettbewerben kann sich eine gute Datenbasis für Programm-Stilometrie ergeben, da hier viele verschiedene Lösungen zu einer einzelnen spezifischen Aufgabe implementiert werden.

03

den USA solche Wettbewerbe und sichern sich die Ergebnisse.

Die Suche nach Programmautoren mit stilometrischen Methoden spielt nicht nur bei der Bekämpfung von Schadsoftware oder bei der Untersuchung potenzieller Urheberrechtsverletzungen eine Rolle. So kann es für Softwareunternehmen interessant sein, zu wissen, ob ihre Mitarbeiter über ein vereinbartes Maß in Open-Source-Projekten mitarbeiten und dabei in Interessenkonflikte geraten. Selbst die Möglichkeit, dass ein Programmierer dies anonym tut, schützt dann seine Privatsphäre nur unzureichend, wenn stilometrische Verfahren Trefferquoten von über 90 % erreichen.

// Manchmal wollen Programmierer nicht als Autoren einer Software erkannt werden. Obfuscation-Software soll Code so verändern, dass er möglichst schwierig zu analysieren ist. Dabei muss jedoch die Semantik des Programms erhalten bleiben.

Obfuscation-Software

Der Erfolg der Analytiker bei der Stilometrie stellt ggf. eine Bedrohung für die Autoren dar – ganz gleich, ob es um die mehr oder um die weniger ehrenwerte Anwendung ihre Könnens geht. Das Ziel, nicht als Autor identifiziert werden zu können, ist damit ein Beweggrund für die Entwicklung von sog. Obfuscation-Software. Deren Aufgabe ist es, Code so zu mischen oder zu verwirren (engl. „obfuscate"), dass er möglichst schwierig zu analysieren ist. Das betrifft sowohl bereits kompilierte Software, bei der das Wiederherstellen des Quelltextes mittels Reverse Engineering erschwert werden soll, als auch Quelltexte oder interpretierten Code, bei dem geistiges Eigentum oder die Autorenschaft geschützt werden soll. Dabei ist in jedem Fall wichtig, dass die Semantik des eigentlichen Programms nicht verändert wird.

Zu den Mitteln, mit denen Obfuscation-Software Verwirrung stiftet, gehören:

- Änderungen des Programmablaufs,
- Einsatz äquivalenter Anweisungen,
- Ergänzung von bedingten Anweisungen oder Sprüngen,
- Zusammenfassen oder Aufteilen von Datenstrukturen,
- Einfügen überflüssigen Codes oder
- Umbenennen von Variablen und Verschlüsseln von Zeichenketten.

Diese und weitere Werkzeuge können das Lesen und Analysieren des Programmcodes sowohl für Menschen als auch für Computer erschweren. Einen sicheren Schutz können sie jedoch nicht bieten.

Bewertung

Öffentliche Verwaltungen setzen eine Vielzahl von Programmen ein. Bei Fachverfahren handelt es sich häufig um individuell erstellte Anwendungen, die im Laufe ihres Lebenszyklus ggf. gepflegt werden müssen. Hierbei sind i. d. R. die Rahmenbedingungen der Erstellung klar definiert. Die Beteiligten sollten im Hinblick auf die Wartung ebenso dokumentiert sein, wie die Weiterverwendbarkeit des Codes durch Programmierrichtlinien unterstützt werden sollte. Trotzdem kann es Fälle geben, in denen die „Entwirrung" von Code oder die Rekonstruktion der Autorenschaft erforderlich ist. Die sachgerechte Analyse dürfte dann aber wohl den Experten auf diesem Gebiet vorbehalten sein. Neben der Anwendung in der Softwareanalyse könnte die Entwicklung der Stilometrie aber auch für den Umgang mit allgemeinen Schriftstücken interessant sein. In der Verwaltung ließen sich so ggf. handelnde Personen anstelle von handelnden Organisationen ermitteln.

STILOMETRIE

Verwaltungsrelevanz:

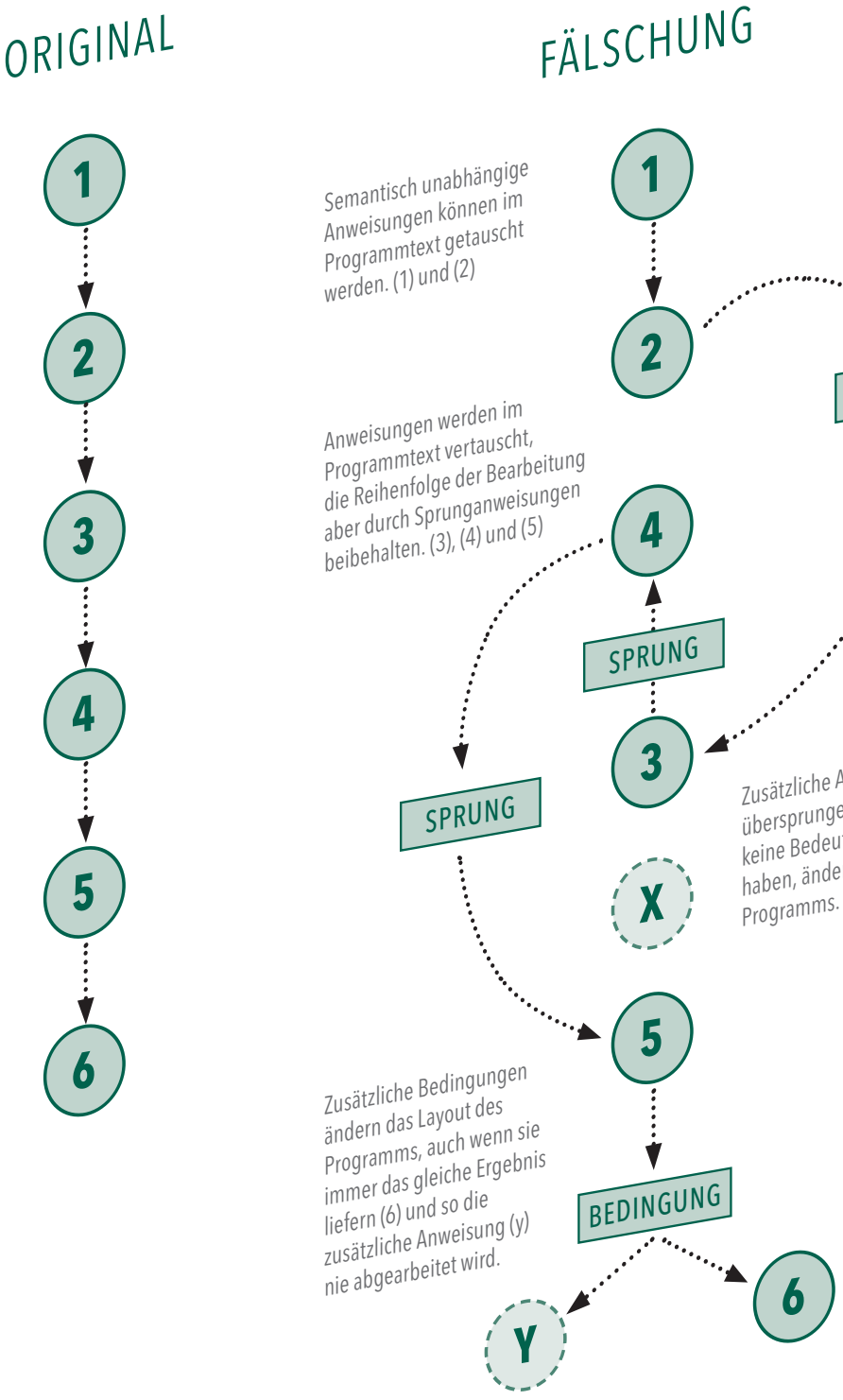
■□□□

Umsetzungs-geschwindigkeit:

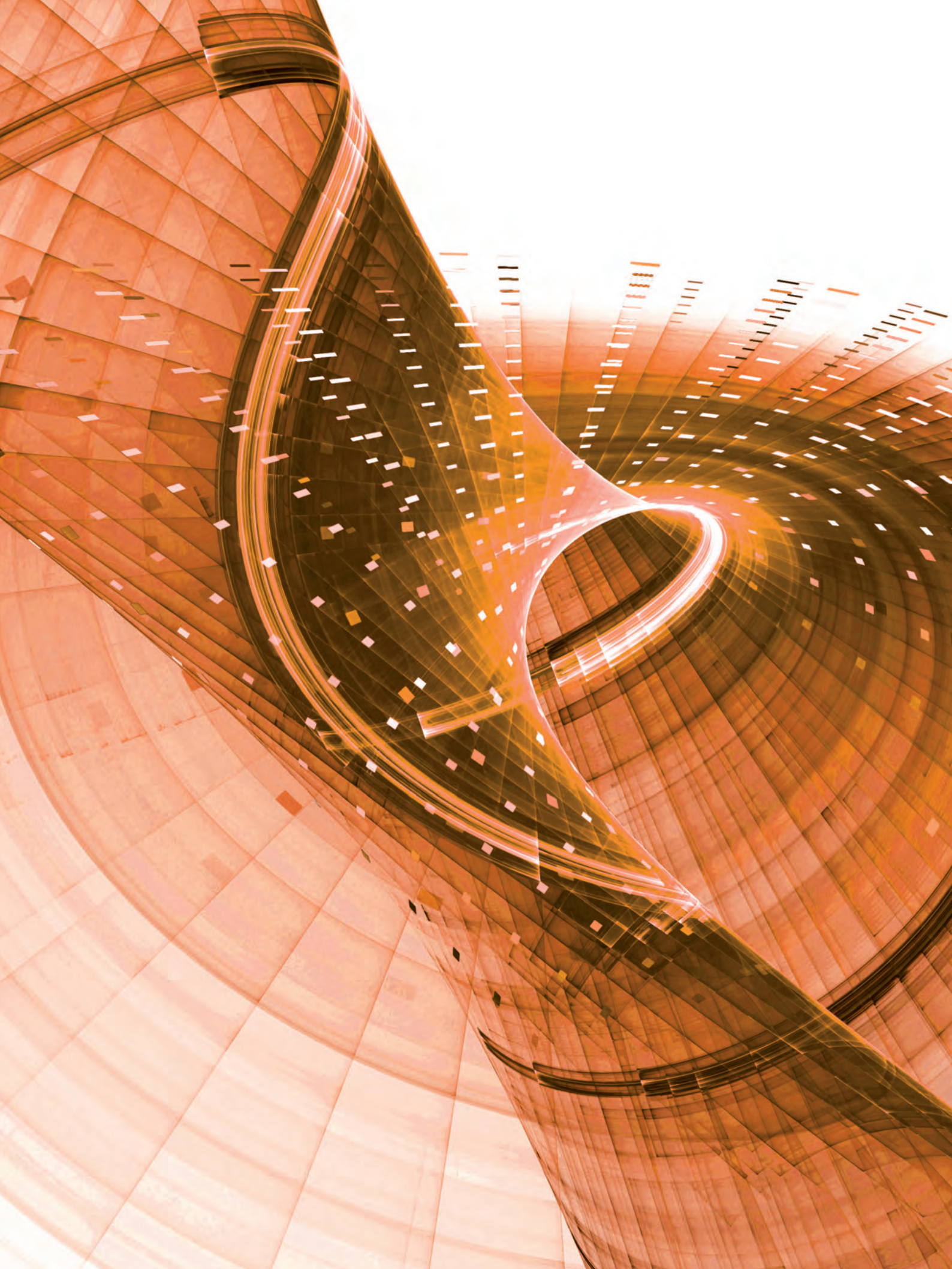
■■■□

Marktreife/Produkt-verfügbarkeit:

■■■■



Obfuscation-Software kann neben geänderten Bezeichnungen und dem Einsatz semantisch äquivalenter Anweisungen auch mit tatsächlichen oder vermeintlichen Änderungen am Programmfluss den Programmierstil verschleiern.



04

GESELLSCHAFT // SICHERHEIT // RECHT

04

DATENSCHUTZHARMONIE

Seit im Jahr 1995 der Datenschutz in der Europäischen Union (EU) mit Hilfe einer Richtlinie geregelt wurde, hat sich im Umgang mit Daten und insbesondere bei deren elektronischer Verarbeitung viel getan. Das gilt nicht nur im Hinblick auf die zunehmende Digitalisierung von Verwaltungen im Rahmen von E-Government-Anwendungen, sondern vor allem im Hinblick auf die zunehmende Erfassung von personenbeziehbaren Daten in allen Lebensbereichen durch privatwirtschaftliche Unternehmen. Viele dieser Unternehmen agieren im Internet und damit i. d. R. weltweit. Das wirft dann z. B. die Frage auf, welches Recht in Streitfragen anzuwenden ist oder welchen Datenschutzregelungen die Daten unterliegen.

// Die „Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG" regelt den Datenschutz in Europa unmittelbar.

Eine EU-Richtlinie hat keine unmittelbare Wirkung, sondern muss zunächst in den Mitgliedstaaten in nationales Recht umgesetzt werden. Das führte dazu, dass beim Datenschutz in der EU unterschiedliche Regelungen galten und in der Folge Unternehmen sich Standorte suchten, die einen aus ihrer Sicht günstigen Rechtsrahmen für die Datenerhebung und -verarbeitung boten. Mit dem Ziel, einerseits die daraus resultierende Wettbewerbsverzerrung zu beheben und andererseits die Rechte von Verbrauchern zu stärken, wurde als Teil der 2012 von der EU-Kommission vorgeschlagenen Datenschutzreform die Erarbeitung einer neuen Datenschutz-Grundverordnung auf den Weg gebracht. Im Unterschied zu einer EU-Richtlinie ist eine EU-Verordnung unmittelbar wirksam und darf in den Mitgliedstaaten grundsätzlich weder verschärft noch abgeschwächt werden – selbst wenn einzelne Details von den Mitgliedern geregelt werden dürfen (s. u.).

Nach langen Verhandlungen des Kommissionsentwurfs und der über 4.000 Änderungsanträge konnte die EU-Verordnung „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)" (DSGVO) am 25. Mai 2016 in Kraft treten. Zunächst läuft jedoch eine zweijährige Übergangsfrist, bis sie zum 25. Mai 2018 wirksam wird.

Einige der für Verbraucher – oder, wie die DSGVO sie nennt, betroffene Personen – wichtigen Regelungen sind folgende Punkte.

Geltungsbereich: Die DSGVO gilt insbesondere für den gesamten privaten und öffentlichen Bereich mit Ausnahme der Sicherheitsbehörden (dort gilt eine spezielle Verordnung). Unternehmen, die in der EU am Markt tätig sind, unterliegen der Verordnung unabhängig davon, ob ihr Sitz in der EU ist bzw. ob die Datenverarbeitung hier stattfindet (Marktortprinzip).

Verbraucherrechte: Die Rechte betroffener Personen bzgl. der Einwilligung in die Verarbeitung, der Auskunft zu erhobenen Daten, der Berichtigung von Daten, der Übertragung von Daten an andere oder des „Vergessenwerdens" wurden in vielen Punkten detailliert geregelt.

Daneben können Klagen gegen Verstöße nun auch bei Gerichten am Aufenthaltsort der betroffenen Person erhoben werden und nicht nur am Sitz des „Verantwortlichen" – sofern es sich bei diesem nicht um eine Behörde handelt, die hoheitlich tätig war. Dabei können sich betroffene Personen auch von Organisationen oder Vereinigungen vertreten lassen. Verstöße gegen das Datenschutzrecht können mit Geldbußen belegt werden, die „wirksam, verhältnismäßig und abschreckend" sind (Art. 83 (1)). Das können bis zu 20 Mio. Euro „oder im Fall eines Unternehmens [...] bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs" sein (Art. 83 (4–6)).

Ein Punkt, bei dem die Mitgliedstaaten abweichende Regelungen festlegen können, betrifft das Mindestalter von Kindern für die Einwilligung in die Verarbeitung personenbezogener Daten. Dieses liegt bei 16 Jahren, kann aber durch Rechtsvorschrift eines Mitgliedstaats dort niedriger – jedoch bei mind. 13. Jahren – liegen (Art. 8 (1)). Ein weiterer solcher Punkt betrifft die Verpflichtung zur Benennung von Datenschutzbeauftragten (Art. 37), die in den Mitgliedstaaten ausgeweitet werden kann.

Die DSGVO war und ist breiter Kritik ausgesetzt. Das wurde bereits an der hohen Anzahl von Änderungsanträgen deutlich und dürfte in der Natur des Harmonisierungsansatzes liegen, der von unterschiedlichen Datenschutz-Niveaus ausstartet: Was an einer Stelle als „unzumutbare" Verschärfung empfunden wird, kann an anderer Stelle als Schwächung des Datenschutzes gesehen werden. Ob man die Anhebung des mittleren Datenschutzniveaus als einen ersten Schritt in die richtige Richtung oder als eine zunehmende Bedrohung von Geschäftsmodellen durch Bürokratisierung einstuft, dürfte von den Zielen der jeweiligen „Verantwortlichen" abhängen.

Bewertung

Auch im öffentlichen Bereich greifen die neuen Rahmenbedingungen der Datenschutz-Grundverordnung. Abgesehen von fachgesetzlichen Regelungen des nationalen Gesetzgebers, die noch erlassen werden müssen und dann umzusetzen sind (Art. 6 (2)), benötigen Behörden ein Datenschutzmanagement von der Planung der Verarbeitung personenbezogener Daten bis hin zum wiederkehrenden Review der eingeführten Prozesse. Erhöhte Anforderungen an die Dokumentation von Datenverarbeitungsvorgängen (z. B. Art. 24, 30, 32), gehen einher mit neuen Verpflichtungen z. B. der Meldung von Datenschutzverstößen an die Datenschutzaufsicht (Art. 33). Entlasten können sich Behörden z. B., indem für gleich gelagerte Datenverarbeitungsvorgänge Verhaltensregeln (Art. 40) erlassen oder Zertifizierungen (Art. 42) angestrengt werden. Behörden sind deshalb gut beraten, wenn sie die bestehenden Rahmenbedingungen, unter denen die automatisierte Verarbeitung personenbezogener Daten erfolgt, vor dem Hintergrund der Datenschutzmanagement-Anforderungen der Verordnung baldmöglichst würdigen. Wie mit Bußgeldern bei Datenschutzverstößen gegenüber Behörden umgegangen wird, ist noch offen. Auch dies bleibt der Entscheidung des nationalen Gesetzgebers vorbehalten (Art. 83 (7)).

DATENSCHUTZ-GRUNDVERORDNUNG

Verwaltungsrelevanz:

Umsetzungsgeschwindigkeit:

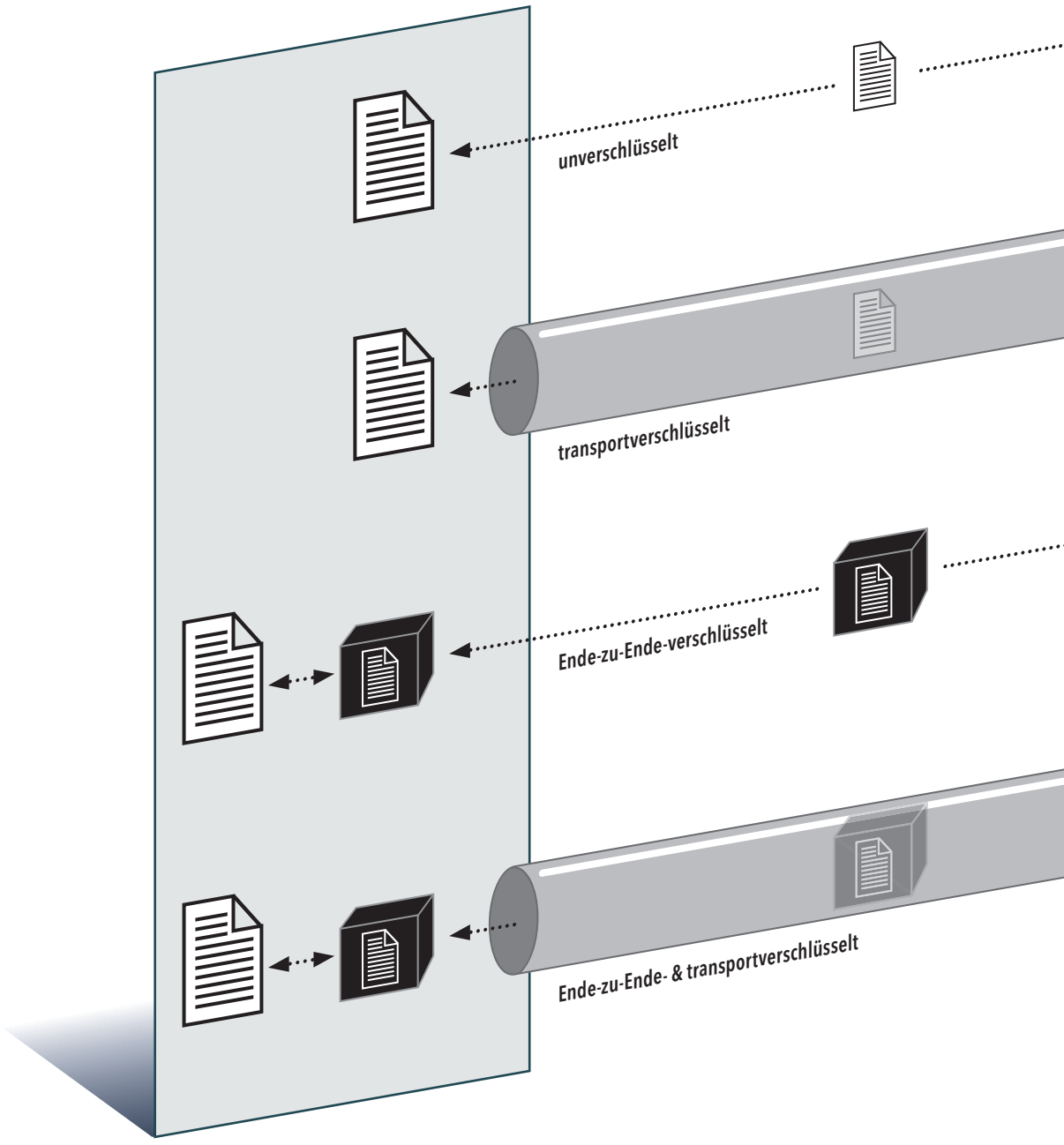
Marktreife/Produktverfügbarkeit:

VOLKSVERSCHLÜSSELUNG FÜR ALLE?

„Es gibt nichts Gutes, außer: Man tut es!" – so hat Erich Kästner es einst treffend formuliert. Und so wird er immer wieder zitiert, wenn es darum geht, dass gute Absichten allein nicht reichen, sondern auch Taten folgen müssen. Auch in puncto IT-Sicherheit kommt es mehr darauf an, was man tatsächlich tut, als was man theoretisch weiß.

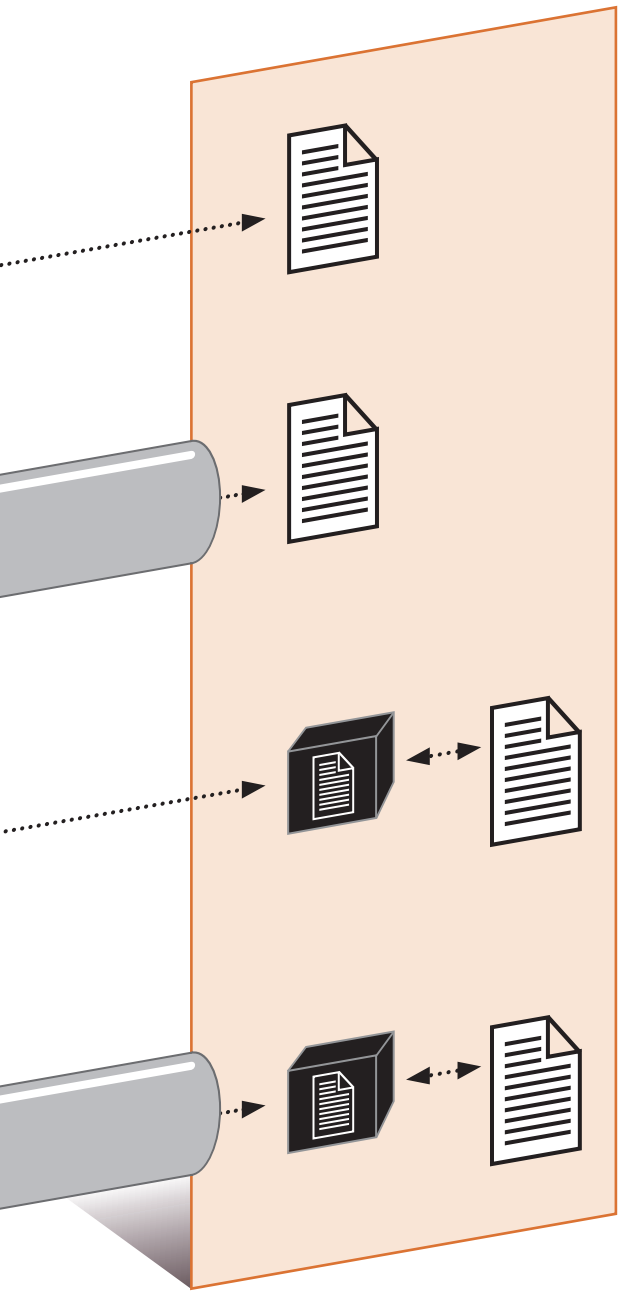
Der Wunsch nach Sicherheit begleitet die Diskussionen um E-Mail, SMS und Kurznachrichtendienste seit Anbeginn der elektronischen Kommunikation. Er wird mal lauter, mal weniger laut artikuliert. Je nachdem, ob Hackerangriffe oder Abhörskandale die Nachrichten beherrschen, oder ob gerade ein neuer, schicker – aber unsicherer – Dienst auf den Markt gekommen ist, den jeder unbedingt nutzen „muss", gestaltet sich der Ruf nach Verschlüsselung der Kommunikation.

Aber nur wenige Nutzer tun auch etwas für diese Art von Sicherheit: Laut einer deutschen IT-Sicherheitsstudie aus dem Jahr 2015 wird nur



Bei der Transportverschlüsselung wird der Übertragungsweg abgesichert. Bei der Ende-zu-Ende-Verschlüsselung wird die Nachricht selbst vor dem Transport codiert.

bei rd. 60 % der E-Mails der Transport durch Verschlüsselung abgesichert; der Anteil der verschlüsselten Nachrichtentexte ist verschwindend gering. Dabei kann nur die sog. Ende-zu-Ende-Verschlüsselung sicherstellen, dass ausschließlich der Absender und der Empfänger die Nachricht ohne weiteres lesen können (s. Abbildung). Oft scheitert die Verwendung von Verschlüsselungssoftware an deren komplizierter Handhabung – sowohl bei der Ein-



richtung als auch bei der Nutzung. Derlei Technik einfach zu gestalten und auch in der breiten Bevölkerung tatsächlich zum Einsatz zu bringen, hat sich das Vorhaben „Volksverschlüsselung" auf die Fahnen geschrieben.

Bei der Verschlüsselung gibt es zwei grundlegende Modelle – die symmetrische bzw. die asymmetrische Verschlüsselung – und deren Mischtechniken. Während bei symmetrischen Verfahren sowohl für die Ver- als auch für die Entschlüsselung einer Nachricht derselbe Schlüssel verwendet wird, werden bei asymmetrischen Verfahren unterschiedliche Schlüssel verwendet – der sog. öffentliche Schlüssel und der private Schlüssel. Hier codiert ein Absender seine Nachricht mit dem öffentlichen Schlüssel des Empfängers. Nur der Empfänger kann diese codierte Nachricht wieder entschlüsseln – und zwar mit Hilfe seines privaten Schlüssels, den er geheimhalten muss. Auf diese Art entfällt die geheime Weitergabe eines Schlüssels, wie sie bei den rein symmetrischen Verfahren erforderlich ist und die ihrerseits hinreichend gut abgesichert werden muss. Da aber die symmetrische Verschlüsselung eine geringere Rechenzeit ermöglicht als die asymmetrische Verschlüsselung, die ihrerseits organisatorisch sicherer ist, werden beide Verfahren in einer sog. hybriden Verschlüsselung kombiniert. Die eigentlichen Daten werden hierbei symmetrisch verschlüsselt. Der genutzte Schlüssel für die symmetrische Verschlüsselung wird hingegen asymmetrisch verschlüsselt übertragen.

Das Schlüsselmanagement bei asymmetrischen Verfahren ist eins der Hindernisse für sichere Mail-Kommunikation: Um eine verschlüsselte Botschaft zu senden, muss der Anwender die öffentlichen Schlüssel seiner potenziellen Adressaten kennen. Wenn er sicher sein will, dass Schlüssel tatsächlich einer bestimmten Person gehören, muss er entweder einer externen

Schlüsselverwaltung vertrauen oder sie selbst verwalten.

Die Volksverschlüsselung ist mit dem Anspruch angetreten, Verschlüsselung in der breiten Bevölkerung zu etablieren. Die Initiative aus Wirtschaft, Forschung und Politik unter Führung des Fraunhofer-Instituts für Sichere Informationstechnologie (SIT) will dies erreichen, indem die entsprechende Technik benutzerfreundlicher wird. So soll auch der Schutz vor Massenüberwachung verbessert werden.

// Die Volksverschlüsselung ist mit dem Anspruch angetreten, Verschlüsselung in der breiten Bevölkerung zu etablieren. Davon verspricht man sich unter anderem mehr Schutz vor Massenüberwachung. Dazu soll vor allem die Technik benutzerfreundlicher werden.

Um die Volksverschlüsselung nutzen zu können, muss zunächst die Identität des Anwenders überprüft werden. Dies kann auf verschiedenen Wegen geschehen, z. B. mittels der eID-Funktion des neuen Personalausweises oder durch persönliche Registrierung beim SIT vor Ort bzw. auf Messen und bei Veranstaltungen. Zudem haben die Kunden eines großen Mailproviders die Möglichkeit, sich über ihr Mailkonto zu registrieren. Nach Feststellung der Identität wird vom SIT ein digitales Zertifikat nach dem Standard X.509, Klasse 3, erstellt, das die Verknüpfung zwischen dem Nutzer und der angegebenen Mailadresse nachweist. Dieses kann dann in Mailclients zum Signieren und Verschlüsseln nach dem Standard S/MIME verwendet werden.

Erste Praxisberichte bestätigen, dass die Handhabung der Volksverschlüsselung tatsächlich einfach sein soll. Somit hätte dieses Verfahren das Potenzial, Sicherheitstechnik in der breiten Bevölkerung zu etablieren. Allerdings wird dieses Potenzial derzeit noch nicht ausgeschöpft, denn es gibt eine ganze Reihe von Rahmenbedingungen, die den Nutzerkreis bzw. die Anwendungsszenarien stark einschränken. Da ist zunächst die Lizenzierung, die sich ausschließlich auf die private Nutzung erstreckt. Mailadressen, die gewerblich oder freiberuflich genutzt werden, dürfen daher nicht mit der Volksverschlüsselung verbunden werden. Dazu kommen technische Einschränkungen. Die kleinste davon dürfte noch die Empfehlung sein, für den Download der Software einen bestimmten Browser zu nutzen, da andere Browser evtl. die Signatur der Anwendung nicht prüfen könnten. Wesentlich schwerer wiegt die Tatsache, dass die Volksverschlüsselung zunächst ausschließlich für Windows-Betriebssysteme verfügbar ist. Andere Betriebssysteme sollen jedoch folgen. Auch die Verwendung der erzeugten Zertifikate auf mobilen Geräten ist nicht ohne weiteres möglich, weil diese die standardkonformen Dateien nicht korrekt verarbeiten können. Diese Hemmnisse machen deutlich, dass nicht die Verschlüsselung an sich schwierig ist. Vielmehr ist es der Anspruch, die Handhabung einfach zu machen, der mit den Herausforderungen heterogener IT-Landschaften konfrontiert wird.

Erschwert werden diese Bestrebungen dadurch, dass es weitere Verschlüsselungsverfahren gibt, die nach anderen Regeln arbeiten. Eins der bekanntesten dürfte Pretty Good Privacy (PGP) sein, aus dem sich der offene Standard OpenPGP entwickelt hat. PGP ist ein hybrides Verfahren (s. o.). Da sich die Formate PGP-codierter Nachrichten, der Schlüssel und Zertifikate von den entsprechenden Gegenstücken bei S/MIME unterscheiden, sind die beiden Verfahren zueinander nicht kompatibel. Dies betrifft also auch die S-MIME-basierte Volksverschlüsselung.

In großen Organisationen – etwa öffentlichen Verwaltungen – existieren oft Strukturen, die für die Registrierung von Anwendern, die Erstellung der benötigten Zertifikate und für deren Validierung zuständig sind. Eine solche Public-Key-Infrastruktur (PKI) kann ggf. über sog. Cross-Zertifizierung mit anderen derartigen Systemen verbunden werden. PKIen mit Zertifikaten auf Basis von X509.3 sind zueinander kompatibel.

So können z. B. Nutzer der Volksverschlüsselung mit Nutzern der HessenPKI sicher Nachrichten austauschen. Ein Hindernis bei der praktischen Arbeit besteht jedoch darin, dass verschiedene PKIen evtl. nicht gegenseitig auf ihre Verzeichnisdienste zugreifen können bzw. ihre eigenen Verzeichnisdienste nicht nutzen, um keine Informationen über Nutzer und die Organisation zu veröffentlichen. Daher müssen Kommunikationspartner bei Bedarf an verschlüsseltem Datenaustausch erst anderweitig Kontakt zueinander aufnehmen und die öffentlichen Schlüssel übermitteln.

Bewertung

Die Volksverschlüsselung mag hinsichtlich der Organisation von Sicherheitstechnik noch nicht der Weisheit letzter Schluss sein. Zu viele offene Fragen stehen einer umfassenden Verwendung in der breiten Bevölkerung noch im Weg. Wenn diese zeitnah geschlossen werden, könnte die Initiative aber tatsächlich dazu beitragen, dass verschlüsselte Nachrichten zum Normalfall in der Mailkommunikation werden. Wer die Volksverschlüsselung – oder andere Verfahren – einsetzt, muss sich jedoch vor Augen führen, welche Möglichkeiten er sich damit erschließt – und welche nicht: Im Fall der konkurrierenden Ziele von Anonymität einerseits und andererseits allgemeiner Authentizität, die nicht auf ungeregelten Vertrauensnetzen basiert, haben sich die Macher der Volksverschlüsselung für Authentizität mit Identitätsnachweis entschieden. Dabei ist jedoch nicht nachvollziehbar, wie sicher mit dem zugehörigen Verzeichnisdienst kommuniziert wird, damit dieses z. B. nicht als Datenquelle verifizierter Adressen für den Spam-Versand genutzt werden kann.

Wenn Verschlüsselung nicht nur in abgegrenzten Bereichen – etwa der Privatanwendung bei der Volksverschlüsselung oder innerhalb spezifischer PKIen – funktionieren soll, müssen Mechanismen geschaffen werden, die die übergreifende Kommunikation einfach ermöglichen. Es reicht dazu nicht aus, verbindliche Krypto-Standards zu definieren. Auch die Handhabung muss einfach und möglichst einheitlich sein. Dann kann man nicht nur über die Notwendigkeit des Verschlüsselns reden, sondern es auch tatsächlich umfassend tun.

VOLKSVERSCHLÜSSELUNG

Verwaltungsrelevanz:

■□□□

Umsetzungsgeschwindigkeit:

■■□□

Marktreife/Produktverfügbarkeit:

■■□□

EIDAS – MIT BRIEF UND SIEGEL

Im Grunde sind sich alle Beteiligten darüber einig, dass elektronischer Geschäftsverkehr sowohl in der Privatwirtschaft als auch im Zusammenwirken mit der öffentlichen Verwaltung immense Vorteile gegenüber einer papiergebundenen Kommunikation hat. Allein Kosten- und Zeitersparnis sprechen klar dafür, noch mehr Informationen über digitale Kanäle auszutauschen. Und dennoch tun sich alle bisherigen Ansätze, diesen Weg gangbar zu machen, schwer, denn trotz der grundsätzlichen Einigkeit der Beteiligten legt jeder einzelne auch besonderen Wert auf verschiedene Aspekte der benötigten Prozesse und Techniken. Für die einen wäre eine schnelle und einfache Kommunikation per herkömmlicher E-Mail – oder gar über proprietäre Kommunikationsdienste – ausreichend, für die anderen geht ohne qualifizierte elektronische Signatur gar nichts. Und dann sind da noch die Belange des Datenschutzes und die Frage nach Verschlüsselung (s. Artikel „Volksverschlüsselung für alle?“).

// Die eIDAS-Verordnung „über elektronische Identifizierung und Vertrauensdienste“ schafft eine Grundlage für die gegenseitige Anerkennung nationaler Vertrauensdienste.

All das unter einen Hut zu bekommen, ist sehr schwierig. Aber untätig will niemand sein. Des-

halb wird an vielen Stellen an den gleichen Themen gearbeitet. Das ist innerhalb Deutschlands so – und das gilt noch mehr, wenn man die europäische Ebene betrachtet. Auch mit viel politischem Willen auf EU-Ebene ist man durchgängigen elektronischen Verwaltungsprozessen mit Instrumenten wie der Signaturrichtlinie (Richtlinie 1999/93/EG) oder der Dienstleistungsrichtlinie (Richtlinie 2006/123/EG) nur wenig nähergekommen.

// eIDAS ist als Verordnung unmittelbar geltendes Recht und muss nicht erst in nationales Recht umgesetzt werden. Eine Lösung, die in einem EU-Mitgliedsstaat anerkannt ist, ist auch in Prozessen der anderen Mitgliedsstaaten verwendbar.

Die EU-Verordnung Nr. 910/2014 „... über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt ..." (eIDAS) ist nun mit dem Ziel der „Beseitigung bestehender Hindernisse bei der grenzüberschreitenden Verwendung elektronischer Identifizierungsmittel, die in den Mitgliedstaaten zumindest die Authentifizierung für öffentliche Dienste ermöglichen" angetreten. Damit wird zwar keine durchgängige technische Lösung für die staatenübergreifende Identifizierung geschaffen. Sie ist aber als Verordnung unmittelbar geltendes Recht und muss nicht erst – wie eine Richtlinie – von den Mitgliedsstaaten in nationales Recht umgesetzt werden. Sie schafft somit eine Grundlage für die gegenseitige Anerkennung nationaler Vertrauensdienste. Das bedeutet, dass eine Lösung, die in einem EU-Mitgliedsstaat anerkannt ist, auch für Prozesse mit dem entsprechenden Sicherheitsniveau in den anderen Mitgliedsstaaten verwendbar ist. Dazu regelt die eIDAS- Verordnung in Artikel 1:

- „Sie legt die Bedingungen fest, unter denen die Mitgliedstaaten elektronische Identifizierungsmittel für natürliche und juristische Personen, die einem notifizierten elektronischen Identifizierungssystem eines anderen Mitgliedstaats unterliegen, anerkennen.
- Sie legt Vorschriften für Vertrauensdienste – insbesondere für elektronische Transaktionen – fest.
- Sie legt einen Rechtsrahmen für elektronische Signaturen, elektronische Siegel, elektronische Zeitstempel, elektronische Dokumente, Dienste für die Zustellung elektronischer Einschreiben und Zertifizierungsdienste für die Website-Authentifizierung fest."

Viel davon klingt vertraut, weil das eine oder andere Hilfsmittel dafür in Deutschland bekannt ist. Signaturen sind z. B. durch das Signaturgesetz geregelt. Ein Dienst für elektronische Einschreiben ist durch das Verfahren De-Mail definiert, sofern dieses mit den Versandoptionen Versandbestätigung, Eingangsbestätigung, absenderbestätigt und persönlich verwendet wird. Neu – und vielleicht mit dem größten Potenzial versehen – ist das Thema elektronische Siegel. Bisher sind für rechtsverbindliche elektronische Vorgänge in Deutschland immer qualifizierte personengebundene Signaturen bzw. Zertifikate erforderlich.

Das elektronische Siegel ist der elektronischen Signatur ähnlich, erlaubt aber die Identifizierung und Zuordnung juristischer Personen. Dadurch werden z. B. Behörden in die Lage versetzt, elektronische Vorgänge als handelnde Organisation zu autorisieren – anstelle der einzelnen Person mit ihrer personengebundenen Signatur.

Die EU-Verordnung definiert die Anforderungen an elektronische Siegel, an fortgeschrittene elektronische Siegel und an qualifizierte elektronische Siegel (Begriffsbestimmung 25., 26. bzw. 27. und Artikel 36) und regelt deren Rechtswirkung (Artikel 35). Bzgl. der Rechtswirkung wird sowohl für elektronische Siegel als auch für die übrigen Instrumente festgeschrieben, dass ihm „die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden [darf], weil es in elektronischer Form vorliegt."

Die für die Anwendung benötigten Vertrauensdienste wie Signaturen, Siegel oder Zeitstempel können von sog. Vertrauensdienstanbietern (VDA) bereitgestellt werden, die sich dafür qualifizieren müssen. Zertifizierte VDA sind an einem Logo erkennbar, das auf einem blauen Vorhängeschloss einen Sternenkranz und ein Häkchensymbol zeigt. Seit dem 1. Juli 2016 müssen die Mitgliedsstaaten der EU ihre zertifizierten VDA gegenseitig anerkennen. Damit ist Stufe 1 der Verordnung in Kraft getreten.

Jedoch erst drei Jahre nach dem Vorliegen von „technischen Spezifikationen, Normen und Verfahren mit Mindestanforderungen" – also ab September 2018 – müssen auch die „elektronischen Identifizierungsmittel" der nationalen Systeme gegenseitig anerkannt werden. Bis dahin müssen die benötigten Dienste auf nationaler Ebene implementiert sein.

Bewertung

Die eIDAS-Verordnung hat das Zeug, die elektronische Kommunikation über Verwaltungsgrenzen hinweg entscheidend voranzubringen. Wenn auf nationaler Ebene Instrumente zur Verfügung stehen, die der Verordnung genügen, dürfte das auch innerhalb der Mitgliedsstaaten zu einer Harmonisierung und Beschleunigung von Prozessen in den Verwaltungen und an der Schnittstelle zu Verwaltungskunden führen. Ein wesentliches Element, das dazu beitragen kann, ist das elektronische Siegel. Für dessen Einsatz sind zwar auch weiterhin spezifische Regelungen zu treffen. Es entfällt aber die aufwändige Bereitstellung personengebundener Signaturen, was die praktische Umsetzung von Zeichnungsbefugnissen wesentlich vereinfachen dürfte. Das Potenzial der Verordnung zur Verbesserung von Verwaltungsvorgängen ist hoch. Es muss aber auch tatsächlich erschlossen werden.

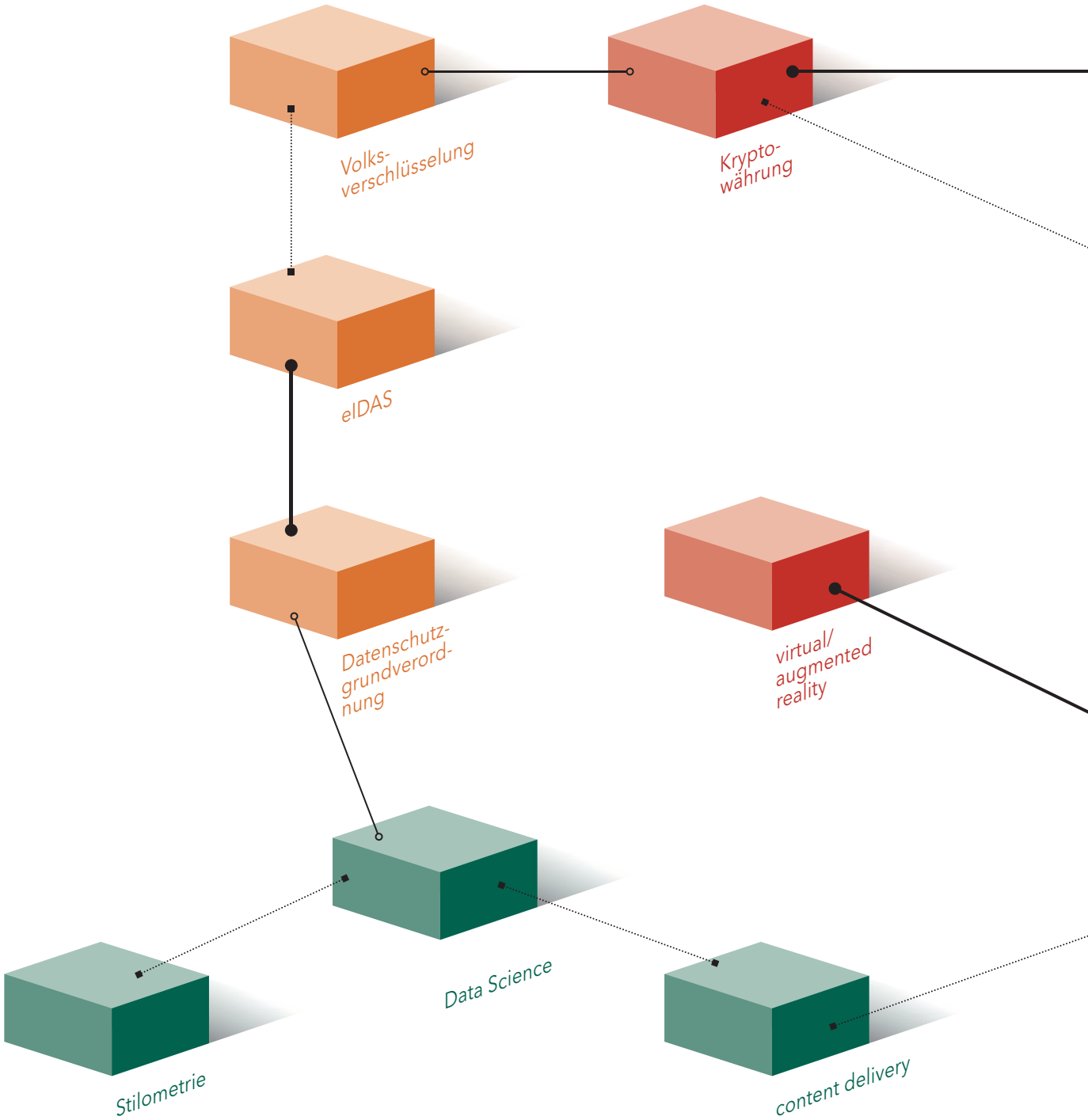
EIDAS – MIT BRIEF UND SIEGEL

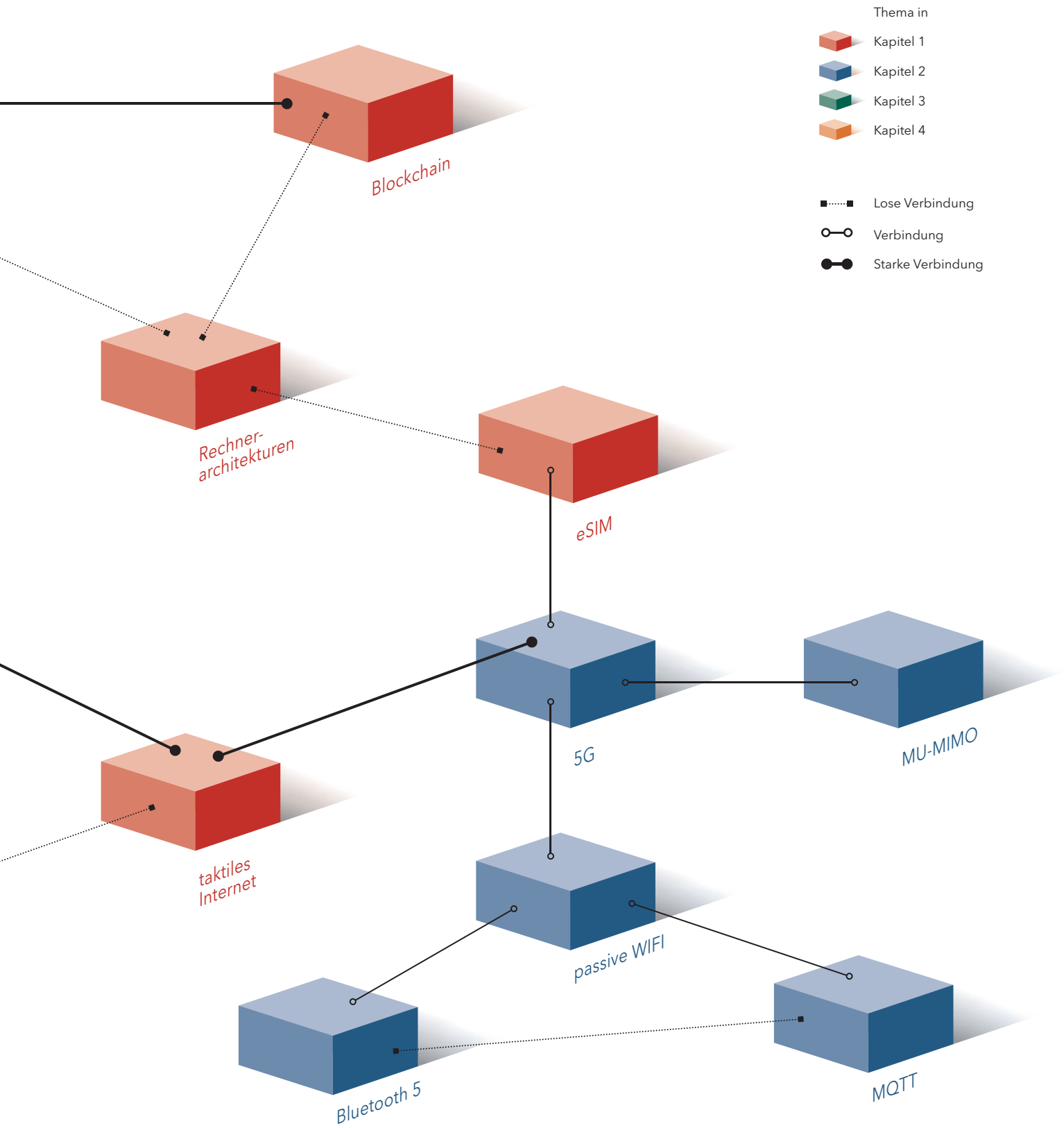
Verwaltungsrelevanz:

Umsetzungsgeschwindigkeit:

Marktreife/Produktverfügbarkeit:

TRENDMAP


Volks-
verschlüsselung
Krypto-
währung
eIDAS
Datenschutz-
grundverord-
nung
virtual/
augmented
reality
Data Science
Stilometrie
content delivery


Thema in
Kapitel 1
Kapitel 2
Kapitel 3
Kapitel 4
Lose Verbindung
Verbindung
Starke Verbindung
Blockchain
Rechner-
architekturen
eSIM
5G
MU-MIMO
taktiles
Internet
passive WIFI
Bluetooth 5
MQTT

IMPRESSUM

Herausgeber
Hessische Zentrale für Datenverarbeitung
Mainzer Straße 29
65185 Wiesbaden
Telefon: 0611 340-0
E-Mail: info@hzd.hessen.de
www.hzd.hessen.de

Verantwortlich
Dr. Markus Beckmann
Telefon: 0611 340-1280
E-Mail: markus.beckmann@hzd.hessen.de

Gestaltung
Agentur 42, Konzept & Design

Kapitelillustrationen
Titel, S. 8/9 ff, S. 40/41 ff, 50/51 ff:
© DrHitch – fotolia.com
S. 28/29 ff:
©phyZick – fotolia.com

Druck
Druckerei Chmielorz GmbH;
www.druckerei-chmielorz.de

Erscheinungstermin
März 2017

ClimatePartner°
klimaneutral
Druck | ID 12360-1702-1001

FSC www.fsc.org
RECYCLED
Papier aus Recyclingmaterial
FSC® C115407

HZD

Mainzer Straße 29 | 65185 Wiesbaden
Telefon: 0611 340-0 | E-Mail: info@hzd.hessen.de
www.hzd.hessen.de