DIV | Deutschland intelligent vernetzt

Digital Gipfel

Dossier Ü-2

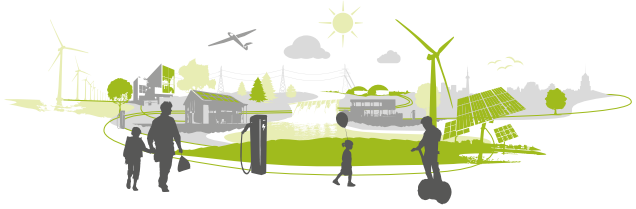
Infrastrukturdaten für neue Geschäftsmodelle

Datenhoheit und -souveränität

Nationaler Digital-Gipfel | Plattform Innovative Digitalisierung der Wirtschaft
Fokusgruppe Intelligente Vernetzung
Dossier der Expertengruppe Intelligente Energienetze

Digital-Gipfel
Plattform Innovative Digitalisierung der Wirtschaft
Fokusgruppe Intelligente Vernetzung

www.deutschland-intelligent-vernetzt.org



1. Zielbild

Der stetig steigende Bedarf an immer intelligenteren Infrastrukturen erfordert auch eine entsprechend stetig mitwachsende Menge an neuen Daten, Informationen und Algorithmen, die einer je nach Anwendung relevanten Sicherheitsstufe unterstehen müssen. Infrastrukturen bilden die Nervenstränge unserer modernen Gesellschaft, damit sind Infrastrukturdaten von hoher Bedeutung für das Zusammenspiel aller gesellschaftlichen Segmente. Um einen reibungslosen Umgang mit allen Infrastrukturen gewährleisten zu können, benötigen diese Infrastrukturen und ihre Daten einen besonderen Schutz. Infrastrukturdaten sind aus unterschiedlichen Gründen sicherheitsrelevant und damit schützenswert und dürfen daher nur sachbezogen genutzt und weiterverarbeitet werden.

Neben der Kritikalität der Infrastrukturdaten bieten sie jedoch auch Möglichkeiten für neue Geschäftsmodelle, die auf diesen Daten gründen. Es gilt, eine Lösung aus Sicht der teilweise hohen Sicherheitsrelevanz für Infrastrukturdaten zu finden, um so die neuen Möglichkeiten der Digitalisierung ausschöpfen und auch Infrastrukturdaten in das Gesamtkonglomerat von öffentlichen und nichtöffentlichen Daten einspeisen zu können. So ist für diesen Spagat eine Lösung zu finden, die sowohl dem Sicherheitsbedürfnis der Infrastrukturdaten als auch den Interessen neuer Geschäftsmodelle nachkommt.

Ein interessanter Ansatz zur Beherrschbarkeit dieser ambivalenten Anforderung – Datensicherheit einerseits, Freigabe der Daten für neue Geschäftsmodelle andererseits – liegt in der Nutzung von sogenannten digitalen Datenzwillingen (digital twins). Bisher werden digitale Datenzwillinge in den Bereichen des Monitorings, der Diagnose und der Prognose verwendet, um die Performance von Assets zu verbessern. Dazu werden neben den „Geburtsdaten“ eines Assets alle Daten seines betrieblichen Lebens gespeichert und zu Optimierungszwecken wie Maintenance-Aufgaben oder Lebensdauerabschätzungen genutzt. Alle Daten eines Assets besitzen einen unterschiedlichen Wert. Somit liegt der Gedanke nahe, die gesammelten Daten im Rahmen eines digitalen Datenzwillings mit einem Index zu versehen, der die Verbreitung dieses jeweiligen Datums einer Infrastruktur regelt. Der digitale Datenzwilling ist somit das eindeutige Abbild einer bestimmten Infrastruktur, in dem der Data Owner im Rahmen seiner Data Governance regelt, welche Daten dieser Infrastruktur an Dritte als Inputparameter für ein neues Geschäftsmodell weitergegeben werden können und welche derart vertraulich oder rechtlich geschützt sind, dass eine Weitergabe auf keinen Fall möglich ist. Voraussetzung für diesen Ansatz eines indizierten digitalen Datenzwillings ist die absolute Unveränderbarkeit des Indexes durch Dritte. Allein der Data Owner hat das Recht und die Möglichkeit, diesen Index zu verändern. Die Datenhoheit ist und bleibt somit beim Data Owner, der in letzter Instanz festlegt, welche Daten er in welcher Form (gar nicht → anonymisiert → pseudonymisiert → offen) einem Geschäftsmodell zur Verfügung stellt.

Diese Daten werden dann auf einer zertifizierten Plattform den Geschäftsmodellen Dritter zur Verfügung gestellt. Über das Kostenmodell wäre an anderer Stelle noch zu befinden.

2. Kurzbeschreibung

Sucht man eine Definition für den Begriff „Infrastruktur“, so lässt sich dieser Begriff gut durch die folgende Erläuterung beschreiben: „Zur Infrastruktur gehören alle staatlichen und privaten Einrichtungen, die für eine ausreichende Daseinsvorsorge und wirtschaftliche Entwicklung als erforderlich gelten. Die Infrastruktur wird meist unterteilt in eine technische Infrastruktur (z. B. Einrichtungen der Verkehrs- und Nachrichtenübermittlung, der Energie- und Wasserversorgung, der Entsorgung) und eine soziale Infrastruktur (z. B. Schulen, Krankenhäuser, Sport- und Freizeitanlagen, Einkaufsstätten, kulturelle Einrichtungen)“.

Insbesondere die technische Infrastruktur bringt mittlerweile eine exponentiell anwachsende Menge an Daten hervor, die zukünftig neben ihrer Nutzung im eigenen Umfeld auch anderen weitergehenden Geschäftsfeldern und Geschäftsmodellen dienen soll. Hierfür bedarf es jedoch Regelungen, die es ermöglichen, diese heute noch vertraulich gehandelten Infrastrukturdaten soweit für Dritte zu öffnen, dass sie sinnvoll nutzbar sind, ohne jedoch missbraucht werden zu können. Gerade aufgrund des Anspruchs an eine ausreichende Daseinsvorsorge spielen Infrastrukturdaten eine wichtige Rolle in unserem täglichen Leben. Dieses Dossier fokussiert sich im Nachfolgenden in seiner Diskussion um den Datenumgang im Schwerpunkt auf Einrichtungen der Verkehrs- und Nachrichtenübermittlung, der Energie- und Wasserversorgung und der Entsorgung. Insbesondere der Einzug der Digitalisierung in allen Lebensbereichen und damit auch in den Bereich der Infrastruktur führt zum Bedarf, für unterschiedliche Anwendungen Infrastrukturdaten nutzen zu wollen. Beispiele hierfür sind infrastrukturübergreifende Anwendungen (Apps) wie Google Maps (nutzt z. B. Handyinformationen zur Stauerkennung) oder Flightradar24 (nutzt Geopositionen von Flugzeugen zur Anzeige auf einer Karte) usw.

Auch der Umbau unseres Energiesystems aufgrund der durch die Bundesregierung beschlossenen Energiewende bringt es mit sich, dass neben dem Anstieg der Dezentralisierung auch die Digitalisierung Einzug in die Energiewirtschaft hält, um alle neuen Vorgänge noch effizienter als in der Vergangenheit bedienen zu können. Insgesamt sind dabei alle Segmente wie Grid, Retail und Renewables gleichermaßen betroffen, neben ihrem Geschäft auch ihre Infrastruktur so zu digitalisieren, dass ihr klassisches Geschäft effizienter abgebildet werden kann. Neben der Verbesserung und Ausweitung des klassischen Geschäftes durch den intelligenten Einsatz von Daten stehen völlig neue Geschäftsmodelle vor der Umsetzung, die sich auf vorhandene, aber auch neue Daten stützen werden. Infrastrukturdaten dienen somit auch in der Energiewirtschaft als Quelle, das „alte“ Geschäft noch besser zu machen und „neues“ Geschäft zu finden. Dabei öffnet sich ein Dilemma, auf der einen Seite sämtliche Infrastrukturdaten nutzen zu wollen, andererseits wichtige Infrastrukturdaten derart geheim zu halten, dass sie nicht durch kriminelle Machenschaften zu missbräuchlichen Anwendungsfällen genutzt werden können.

Wir benötigen daher für Deutschland ein Grundkonzept, das die Bereitstellung und Nutzung von Infrastrukturdaten klar regelt. Dabei soll dieses Grundkonzept auf keinen Fall schützenswerte Daten öffnen, aber auch nicht Infrastrukturdaten zurückhalten, die für neue Geschäftsmodelle sinnvoll eingesetzt werden können. Dabei werden die klassischen Monopolstellungen der Infrastrukturbetreiber aufgebrochen und aus der altbekannten Wertschöpfungskette wird eher ein Wertschöpfungsnetzwerk, in dem sich eine Vielzahl von neuen Marktakteuren tummeln wird. Nur wie kann nun erreicht werden, beiden „Herren“, nämlich dem Bedarf an mehr öffentlicher Transparenz und Nutzbarkeit von Infrastrukturdaten und dem Bedarf nach Schutz von sicherheitsrelevanten Infrastrukturdaten, zu dienen?

Interpretiert man die Gesamtheit aller Infrastrukturdaten als ein neues Ökosystem, dann wird sehr schnell deutlich, dass Infrastrukturdaten ein unterschiedliches Sicherheitsbedürfnis besitzen und einer Schutzbedarfsfeststellung unterliegen.

Wie bei personenbezogenen Daten sinkt auch bei Infrastrukturdaten das Sicherheitsbedürfnis, wenn sie anonymisiert oder pseudonymisiert wurden. Wichtig bei

der Weitergabe von sicherheitsrelevanten Infrastrukturdaten ist die Verklärung des direkten Bezugs auf das jeweilige Infrastrukturobjekt.

Um Infrastrukturobjekte beschreiben zu können, hat sich der Begriff eines „digitalen Datenzwillings" eingebürgert, der bedeutet, dass jedes Objekt einen zweiten digitalen Datensatz besitzt, der in einem Computersystem gespeichert ist. Ein digitaler Zwilling bezieht sich auf ein computergestütztes Modell eines materiellen oder immateriellen Objekts, welches für verschiedene Zwecke verwendet werden kann. Dieser digitale Datenzwilling bildet das jeweilige Infrastrukturdatenobjekt 1:1 ab. Damit ist es möglich, je nach Sicherheitsbedürfnis des jeweiligen Infrastrukturdatums dieses vor einer Weitergabe an Dritte über eine Indizierung zu verhindern, zu verklären oder zu erlauben. Diese Indexvergabe obliegt einzig und allein dem Data Owner, der sowohl für das Infrastrukturdatum selbst als auch die Indizierung die komplette Datensouveränität besitzt.

3. Diskussionsperspektiven

Contra: Infrastrukturdaten unterliegen im Wesentlichen einer derartigen Kritikalität (KRITIS[1]), dass sie auf keinen Fall außerhalb ihrer eigentlichen Umgebung für neue Geschäftsmodelle genutzt werden dürfen.

Infrastrukturdaten unterliegen einer hohen Kritikalität. Die Datenhoheit liegt beim jeweiligen Infrastrukturbetreiber, er ist – auch aus gesetzlicher Sicht – für die Sicherheit der Infrastruktur und damit auch für die Infrastrukturdaten verantwortlich. Mögliche Geschäftsmodelle können daher nicht mit Daten aus dem Infrastrukturumfeld versorgt werden. Zudem ist eine Indizierung und damit eine Priorisierung der Daten über einen digitalen Zwilling aufwendig und nicht sicher umsetzbar. Das Risiko eines Missbrauches von Infrastrukturdaten steht in keinem Verhältnis zu einem neuen Geschäftsmodell, das aus dem Pool von Infrastrukturdaten versorgt wird. Neue Geschäftsmodelle, die sich auf Infrastrukturdaten beziehen wollen, müssen bestenfalls mit pseudonymisierten Daten auskommen oder mit Abschätzungen arbeiten.

Pro: Auch sicherheitsrelevante Infrastrukturdaten lassen sich durch geeignete Verfahren wie z. B. der Indizierung über einen digitalen Zwilling oder durch Anonymisierung/Pseudonymisierung so aufbereiten, dass sie bedenkenlos auch außerhalb ihrer eigentlichen Umgebung zur Unterstützung neuer Geschäftsmodelle an Dritte weitergegeben werden können.

Die digitale Transformation der Gesellschaft erfordert einen deutlichen Paradigmenwechsel in der Datenpolitik. Daten sind der zentrale Rohstoff der digitalen Wirtschaft. Damit sind auch Daten öffentlicher Infrastrukturen nicht mehr allein Sache der Infrastrukturbetreiber, Infrastrukturdaten müssen auch Dritten in einer geeigneten Form zur Verfügung gestellt werden, um aus ihnen neue Geschäftsmodelle entwickeln zu können. Natürlich sind Datensicherheit und Datensouveränität wichtige Grundpfeiler für die Akzeptanz und den Erfolg einer datengetriebenen Ökonomie. Es gibt heute jedoch Verfahren, die es ermöglichen, dass alle rechtlichen Vorgaben und auch die Datensouveränität der Data Owner eingehalten werden können.

Neben der Anonymisierung und Pseudonymisierung gibt es Möglichkeiten, über eine Indizierung des digitalen Zwillings nur die Infrastrukturdaten den neuen Geschäftsmodellen bereitzustellen, die der Data Owner freigibt. Infrastrukturbetreiber haben so die Möglichkeit, aus den zur weiteren Nutzung bereitgestellten Daten zusätzliche Gewinne zu erzielen.

Hinsichtlich der Datenhaltung von Infrastrukturdaten lassen sich BSI-zertifizierte Rechenzentren einsetzen, die einen Angriff durch Dritte erst gar nicht ermöglichen. Somit sind die hier abgelegten Infrastrukturdaten sicher.

1 https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2017/06/nis-richtlinie.html

4. Handlungsempfehlungen

1. Um eine Differenzierung von Infrastrukturdaten in „öffentliche“ und „nicht öffentliche“ Daten herstellen zu können, ist es notwendig, im Einvernehmen mit staatlichen Stellen ein geeignetes Verfahren zur Indizierung von Einzeldaten herzustellen. Mit Hilfe dieses Verfahrens ist der Data Owner Herr der Lage, seine Datensouveränität auszuüben. Eine hierfür mögliche Lösung kann in der Indizierung der Infrastrukturdaten im digitalen Zwilling liegen.
2. Alle Infrastrukturdaten, die einer Weiterverwendung durch Dritte zugeführt werden sollen, müssen über eine zertifizierte Institution (z. B. ein BSI-zertifiziertes Rechenzentrum) zur Verfügung gestellt werden. Damit wird erreicht, dass der Data Owner seine Datensouveränität behält und „seine“ Infrastrukturdaten gegenüber der Manipulation durch Dritte geschützt werden. Anreize für die Bereitstellung von Infrastrukturdaten sind zu prüfen.
3. Der Gesetzgeber muss es den Infrastrukturbetreibern ermöglichen, weniger kritische Daten über ein BSI-zertifiziertes Rechenzentrum bereitzustellen. Der Infrastrukturbetreiber ist somit in der Lage, Teile seiner Daten an Dritte zu verkaufen.
4. Infrastrukturbetreiber müssen sich mit der Sachlage auseinandersetzen, Teile ihrer Infrastrukturdaten Dritten für eine Weitervermarktung bzw. Weiternutzung in Applikationen zu überlassen. Die Infrastrukturbetreiber versetzen sich so auch selbst in die Lage, ihre eigenen Infrastrukturrohdaten in eigenen Applikationen zu verwenden und diese Applikationen Anwendern zur Verfügung zu stellen.

5. Referenzen

– BNetzA: Konsultation der Bundesnetzagentur zur Einrichtung der zentralen Informationsstelle des Bundes auf Grundlage der §§ 77a und 77b TKG 2016. Umsetzungskonzept für den Infrastrukturatlas für Planungszwecke und Mitnutzungen
– Ein Internet-Kennzahlensysten für Deutschland: Anforderungen und technische Maßnahmen; Sebastian Feld, Tim Perrei, Norbert Pohlmann, Matthias Schupp, Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen
– Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie); Bundesministrium des Innern
– Analytics: Big Data in der Praxis. Wie innovative Unternehmen ihre Datenbestände effektiv nutzen; IBM Business Services, IBM Institute for Business Value; Business Analytics and Optimization in Kooperation mit der Said Business School an der Universität Oxford

Ansprechpartner

Prof. Dr.-Ing. Michael Laskowski, innogy SE
Hinnerk Fretwurst-Schiffel, T-Systems International GmbH

Fokusgruppe Intelligente Vernetzung im Nationalen Digital-Gipfel / Expertengruppe Intelligente Energienetze

Alle Dokumente und Publikationen kostenlos zum Download:

www.deutschland-intelligent-vernetzt.org