Bundesministerium des Innern

Sicherheitsaspekte bei der Umsetzung von INSPIRE[1] durch Ver- und Entsorgungsunternehmen

Die von der INSPIRE-Richtlinie betroffenen Geodaten von Infrastrukturen von Ver- und Entsorgungsunternehmen haben zum Teil sensiblen Charakter. Als ein Beispiel seien hier Geodaten zu Leitungsnetzen und Hydranten genannt. Dies gilt umso mehr, wenn es sich bei den Anlagen der Ver- und Entsorgung um Kritische Infrastrukturen handelt. Die Transparenzziele und -auflagen der INSPIRE-Richtlinie dürfen daher nicht in Widerspruch zu den Zielen und Maßnahmen zum Schutz Kritischer Infrastrukturen stehen. Betreiber Kritischer Infrastrukturen wurden im Juli 2015 mit dem IT-Sicherheitsgesetz zu mehr Sicherheit hinsichtlich ihrer IT verpflichtet.
Wie für alle anderen geodatenhaltenden Stellen besteht auch für die Betreiber Kritischer Infrastrukturen die Pflicht zu INSPIRE-konformer Vorhaltung der Geodaten sowie dazu, autorisierten Bedarfsträgern mit berechtigtem Interesse Zugang zu gewähren. Geodaten von Infrastrukturen, deren Veröffentlichung keine Gefährdung für die öffentliche Sicherheit mit sich bringt, werden wie alle anderen Geodaten entsprechend den Vorgaben der INSPIRE-Richtlinie durch die geodatenhaltende Stelle für die Öffentlichkeit bereitgestellt.
Für sensible Geodaten ist in der INSPIRE-Richtlinie und den Geodatenzugangsgesetzen des Bundes und der Länder eine Ausnahme vorgesehen: Die geodatenhaltenden Stellen unterliegen zwar der Richtlinie, müssen jedoch sensible Geodaten nicht für jedermann zugänglich machen. Sofern der Zugang der Öffentlichkeit zu den betreffenden Geodaten entsprechend Art. 13 Abs. 1 INSPIRE-Richtlinie nachteilige Auswirkungen auf die öffentliche Sicherheit hat, kann der Zugang für die allgemeine Öffentlichkeit sowohl zu den Suchdiensten, und damit auch zu den Metadaten, als auch zu den Darstellungs- und Downloaddiensten beschränkt werden. So sieht die Ausnahme gemäß Art. 13 Abs. 1 eine Beschränkung des Zugangs vor, jedoch nicht die Befreiung von der Pflicht, INSPIRE-konforme Metadaten und Geodaten an sich vorzuhalten. Daher müssen Wege gefunden werden, um die Daten für einen (voraussichtlich kleinen) Personenkreis mit berechtigtem Interesse zugänglich zu machen. Auch die Pflicht zur Meldung der INSPIRE-relevanten Daten und Dienste aller nationalen geodatenhaltenden Stellen im jährlichen Monitoring ist davon unberührt.

Die Geodaten und Dienste selbst verbleiben im Rahmen der INSPIRE-Umsetzung grundsätzlich bei den geodatenhaltenden Stellen (vgl. Grundsatz der GDI-DE der „Dezentralität der Geodaten“, s. Architekturkonzept V.3.1). Dem berechtigten Nutzer wird der Zugang zu den Geodaten über Darstellungs- und Downloaddienste durch den Datenhalter zur Verfügung gestellt. Die geodatenhaltende Stelle entscheidet über den Zugang zu ihren Daten, insbesondere sofern diese als sicherheitskritisch eingestuft werden.

[1] Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft

Für den Umgang mit sensiblen Geodaten bedeutet dies, dass der Zugang zu Metadaten, Geodaten und -diensten Kritischer Infrastrukturen nach der INSPIRE-Richtlinie für die allgemeine Öffentlichkeit zu beschränken bzw. zu versagen ist. Im Falle der Zugänglichkeit dieser Geodaten würde die Zielvorgabe des IT-Sicherheitsgesetzes, die Funktionsfähigkeit Kritischer Infrastrukturen zu gewährleisten, konterkariert, weil potenziellen Angreifern der Angriff auf Kritische Infrastrukturen erst ermöglicht würde. Wenn Kritische Infrastrukturen betroffen sind, liegen daher nachteilige Auswirkungen auf bedeutsame Schutzgüter der öffentlichen Sicherheit im Sinne von § 12 Abs. 1 Geodatenzugangsgesetz (GeoZG) und den entsprechenden Landesgesetzen vor. Ausschließlich für autorisierte Bedarfsträger, wie beispielsweise Polizei, Bundeswehr oder Katastrophenschutzeinrichtungen, müssen geeignete Mechanismen - wie auch nach dem IT-Sicherheitsgesetz gefordert - gefunden werden, um die Daten zu schützen und gleichzeitig die rechtlichen Vorgaben nach INSPIRE zu erfüllen. Entsprechend den Vorgaben nach §8 a Abs. 2 BSI-Gesetz sollten die Betreiber der Kritischen Infrastrukturen und ihre Branchenverbände geeignete branchenspezifische Möglichkeiten vorschlagen.

Für Betreiber Kritischer Infrastrukturen muss unter Bezug auf § 13 Abs. 1 INSPIRE-Richtlinie und § 12 Abs. 1 GeoZG und den entsprechenden Landesgesetzen zur Vermeidung nachteiliger Auswirkungen auf die öffentliche Sicherheit gelten:

1. Der Zugang zu Geodaten (Geodatensätze und -Dienste) und Metadaten wird für die Öffentlichkeit beschränkt, wenn durch deren Veröffentlichung die öffentliche Sicherheit gefährdet ist.

2. Eine Gefährdung liegt in jedem Fall vor, wenn Infrastrukturen betroffen sind, die durch Gesetz oder aufgrund eines Gesetzes als Kritische Infrastrukturen gelten.

3. Unabhängig von der Kritikalität einer Infrastruktur ist darüber hinaus eine Gefährdung in der Regel zu vermuten, wenn Geodaten schutzbedürftige Komponenten der jeweiligen Infrastruktur betreffen.

4. Die Prüfung der Schutzbedürftigkeit von Komponenten erfolgt durch den Betreiber.

5. In den Metadaten ist die Beschränkung des Zugangs kenntlich zu machen.