Bundesverband
Breitbandkommunikation e.V.

Berlin, 31.01.2024

Dezentraler Infrastrukturatlas – Ein Strategiepapier zur sicheren und effizienten Verwaltung von Infrastrukturinformationen

Ein Strategiepapier des BREKO Bundesverband Breitbandkommunikation e.V.

Management Summary

Telekommunikationsnetze (TK-Netze) gehören zur kritischen Infrastruktur und können Ziel von Angriffen und Sabotage sein. Daher haben Informationen über diese Infrastruktur einen besonderen Schutzbedarf. Der Infrastrukturatlas (ISA) der Bundesnetzagentur wird dem Erfordernis eines angemessenen Schutzes der Daten über kritische Infrastruktur nicht hinreichend gerecht, weshalb der Bundesverband Breitbandkommunikation e. V. (BREKO) eine Weiterentwicklung und Verbesserung als erforderlich ansieht. Durch die Etablierung einer dezentralen statt zentralen Datenhaltung könnten Risiken für die Sicherheit der Kritischen Infrastruktur minimiert werden, indem die Datenhoheit bei den Dateninhabenden Unternehmen verbleibt. Zudem wird eine erhöhte Transparenz über den Datenzugriff und die Datennutzung geschaffen. Daneben würden durch eine dezentrale Datenhaltung Effizienzpotenziale im Glasfaserausbau durch Aktualität und automatisierte Prozesse gehoben werden.

Die wesentlichen Aspekte des Konzeptes eines dezentralen Infrastrukturatlas (dISA) sind

- eine dezentrale Haltung von Infrastrukturdaten sowie die durchgängige Nutzung von modernen Verschlüsselungstechnologien und Authentifizierungsmechanismen, um den Anforderungen an die Informationssicherheit gerecht zu werden,
- eine Reduzierung des Datenaustauschs auf den erforderlichen Umfang und die benötigte Genauigkeit,
- ein automatisiertes Verfahren zur Aktualisierung der Infrastrukturinformationen, um den Anforderungen nach Aktualität gerecht zu werden,
- eine vollständige Digitalisierung aller mit dem ISA verbundenen Prozesse, um eine deutliche Steigerung der Effizienz im Glasfaserausbau zu erreichen.

Mit dem vorliegenden Konzept eines dezentralen Infrastrukturatlas wird ein wesentlicher Schritt im Sinne einer sicheren Digitalisierung gegangen, mit dem den Verpflichtungen bzgl. der Informations- und Datenbereitstellung aus den einschlägigen Regelungen (TKG, GIA, Kostensenkungsrichtlinie für den Breitbandausbau, Europäischer Kodex für elektronische Kommunikation) sowie den Anforderungen an eine hohe Resilienz und Sicherheit (KRITIS-DG, NIS2-Umsetzungsgesetz) Rechnung getragen würde.

1. Einleitung

Der Infrastrukturatlas (ISA) der Bundesnetzagentur, auch bekannt als ISA, ist ein zentrales Informations- und Planungsinstrument für den Ausbau von Gigabitnetzen in Deutschland. Betrieben wird er von der zentralen Informationsstelle des Bundes (ZIS) der Bundesnetzagentur. Der ISA ist im Telekommunikationsgesetz (TKG) verankert und bietet umfangreiche Daten zu verschiedenen Infrastrukturen, die von Eigentümern und Betreibern öffentlicher Versorgungsnetze sowie sonstiger physischer Infrastrukturen bereitgestellt werden. Somit enthält er Daten von über 3.500 Infrastrukturinhabern und macht diese Informationen für Unternehmen sowie staatliche Ebenen wie den Bund, Länder und Kommunen im Rahmen des Gigabitausbaus zugänglich.

Im Rahmen der Gigabitstrategie der Bundesregierung sind eine Reihe von Erneuerungen und Erweiterungen des ISA, der Teil des sogenannten Gigabit-Grundbuchs geplant, welche die Nutzung und den Mehrwert des ISA verbessern sollen.

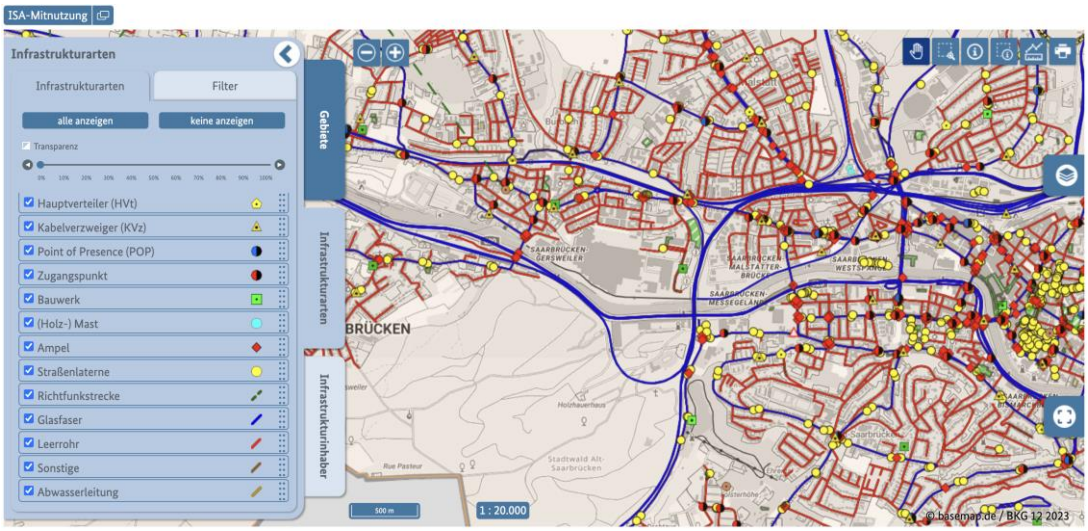

Abbildung 1: Darstellung von Infrastrukturdaten im Infrastrukturatlas

Nichtsdestotrotz sieht der BREKO, dass insbesondere die gestiegenen Sicherheitsanforderungen – hierzu zählen die durchgängige Nutzung von Verschlüsselung, Zwei-Faktor-Authentifizierung und Maßnahmen zur Erkennung von Missbrauch – nicht erfüllt werden. Darüber hinaus gibt es aber auch weitere Anforderungen der Nutzungsgruppen des ISA (siehe Kapitel 3), deren Berücksichtigung auf einen effizienteren und effektiveren Netzausbau einzahlen würden.

Daher wollen wir mit diesem Strategiepapier die Diskussion über wesentliche Aspekte des ISA eröffnen und ein Lösungskonzept für einen verbesserten und *dezentralen Infrastrukturatlas* (dISA) vorlegen.

Dieses Konzept erfüllt die notwendigen Kriterien der Informationssicherheit für Kritische Infrastruktur, die Anforderungen der beteiligten Unternehmen im Sinne von Effizienz und Aktualität. Es entspricht zudem den Vorgaben der Kostensenkungsrichtlinie für den Breitbandausbau (KSRL)bzw. des geplanten Gigabit Infrastructure Act (GIA) und dem Kodex für die elektronische Kommunikation der EU nach sicherer, zentraler Bereitstellung von Infrastrukturinformationen und ermöglicht dadurch einen effizienteren und effektiveren Ausbau. Als Orientierung für das Konzept dienen die in Dänemark etablierten Systeme zur Registrierung[1] von Infrastruktur und Beantragung[2] von Baumaßnahmen, die ebenfalls die Anforderungen des GIA berücksichtigen. Der dISA verfolgt die Paradigmen „Minimierung der Information auf das Notwendige“ (Need-to-Know-Prinzip[3]) und „Maximierung der Effizienz durch Digitalisierung“.

Da das Gigabit-Grundbuch eine Reihe von Funktionalitäten in einem Portal zusammenfasst, wird mit diesem Papier aber ausschließlich die Funktionen des heutigen ISA betrachten, werden im Folgenden immer die Begriffe „Infrastrukturatlas“ beziehungsweise „ISA“ verwendet.

2. Motivation

Die Motivation, die Diskussion um Änderungen und Erweiterungen des ISA zu beginnen, entspringt drei wesentlichen Aspekten, die sich aus den Anforderungen der Nutzenden des ISA herauskristallisieren:

- Informationssicherheit

[1] LER – Register of Underground Cable Owners (graveinfo.ler.dk)

[2] Tjekditnet.dk: der dänische Breitbandatlas

[3] Need-to-Know-Prinzip, analog zur DSGVO wird sowohl der Kreis derjenigen, die Zugang zu den Daten haben, auf solche mit einem berechtigten Interesse begrenzt, als auch die Menge der Informationen, die der Berechtigte für die Ausführung seiner Tätigkeiten benötigt.

- Effizienz und Effektivität
- Automatisierung und Transparenz

Im Folgenden werden diese Anforderungen detailliert betrachtet.

2.1. Informationssicherheit

In Zeiten wachsender krimineller Angriffe gegen staatliche Stellen und Unternehmen stellen Infrastrukturen ein extrem gefährdetes und damit besonders schützenswertes Gut dar. Die Beispiele der Attacken gegen die Infrastruktur der Deutschen Bahn im Oktober 2022 und September 2023 zeigen eindrücklich, wie leicht verwundbar die Kommunikationsnetze sind und welchen Einfluss und Schaden solche Attacken haben können.

TK-Netze sind Teil der Kritischen Infrastruktur der Bundesrepublik Deutschland. Sie spielen eine zentrale Rolle für die digitale Kommunikation und die Digitalisierung.

- Sie bilden das Rückgrat moderner Kommunikationstechnologien, ermöglichen Hochgeschwindigkeitsinternet, was für private, geschäftliche, bildungsbezogene und staatliche Aktivitäten unerlässlich ist. Insbesondere in unserer zunehmend digitalisierten Welt ist der Zugang zu schnellem und zuverlässigem Internet eine Grundvoraussetzung für zahlreiche tägliche Prozesse und digitale Teilhabe.
- Ihre wirtschaftliche Bedeutung steht außer Frage. Eine leistungsstarke Telekommunikationsinfrastruktur ist entscheidend für die Wirtschaft eines Landes. Unternehmen aller Größen sind auf schnelle und zuverlässige Internetverbindungen angewiesen, um wettbewerbsfähig zu bleiben. Dies gilt insbesondere für Branchen, die auf Cloud-Dienste, E-Commerce, Fernarbeit (Home-Office) und digitale Kommunikation angewiesen sind.
- TK-Netze haben eine wesentliche Bedeutung für die öffentliche Sicherheit und Gesundheit. Kommunikationsnetze sind entscheidend für die Funktionsfähigkeit von Notdiensten und Gesundheitseinrichtungen. Sie ermöglichen die schnelle Koordination bei Notfällen und Katastrophen und stellen sicher, dass lebenswichtige Informationen effektiv übermittelt werden können.
- Andere Kritische Infrastrukturen sind abhängig von TK-Netzen. Sie sind nicht nur für sich genommen wichtig, sondern auch, weil sie andere Kritische Infrastrukturen wie Energieerzeugungsanlagen, Verkehrssysteme und staatliche Dienste unterstützen. Diese Systeme sind zunehmend vernetzt und abhängig von einer stabilen und schnellen Internetverbindung.
- Wie jede wichtige Infrastruktur sind auch TK-Netze potenziellen Bedrohungen durch natürliche Katastrophen, technische Ausfälle oder böswillige Angriffe ausgesetzt. Die Vergegenwärtigung, dass es sich bei jener Infrastruktur um Kritische Infrastruktur handelt, ist daher wichtig, um das Bewusstsein für das Erfordernis einer erhöhten Resilienz zu stärken und notwendige Sicherheitsmaßnahmen durchzusetzen.
- In einer Zeit, in der Daten als neues "Öl" gelten, ist der Schutz und die sichere Übertragung von Daten und die digitale Souveränität von höchster Bedeutung. IKT-Netze spielen dabei eine Schlüsselrolle, sowohl in Bezug auf die Geschwindigkeit als auch auf die Sicherheit der Datenübertragung.
- Nicht zuletzt haben TK-Netze eine soziale und kulturelle Bedeutung. Der Zugang zu Informationen und Bildung sowie die Teilnahme am kulturellen und sozialen Leben sind zunehmend digitalisiert. TK-Netze ermöglichen eine breite und gleichberechtigte Teilhabe an diesen gesellschaftlichen Aspekten.

All diese Aspekte begründen ein grundsätzliches Umdenken beim Umgang mit Informationen über Telekommunikationsinfrastrukturinformationen, um Missbrauch und potenzielle Bedrohungen schon im Ansatz zu erschweren.

Die derzeitige zentrale Haltung von zum Teil sehr detaillierten Infrastrukturdaten im ISA sowie die Tatsache, dass Zugänge nicht mit modernen Technologien (z. B. Zwei-Faktor-Authentifizierung) und systematisch abgesichert sind, stellt ein erhebliches Risiko dar. Innerhalb der Gigabit Strategie der Bundesregierung finden sich zwar einige Maßnahmen zur Optimierung von Prozessen, bzgl. einer deutlichen Erhöhung der Informationssicherheit finden sich allerdings keine Angaben.

Ähnlich wie beim Datenschutz, sollte mehr als zuvor darauf geachtet werden, dass nur die unbedingt notwenigen Informationen übermittelt bzw. gespeichert werden, der Zweck der Abfrage und Nutzung genau bestimmt ist, die verarbeitenden Stellen für Eigner der Informationen transparent sind und eine Löschung der Informationen nach Ende des Nutzungszwecks bzw. Frist durchgeführt wird.

2.2. Effizienz und Effektivität

Der Ausbau von Glasfasernetzen in Deutschland schreitet trotz zahlreicher Herausforderungen stetig voran. So konnte im Jahr 2023 bereits eine Glasfaserquote von 35 Prozent erzielt werden. Um das Ziel eines flächendeckenden Ausbaus von Glasfasernetzen bis zum Jahr 2030 erreichen zu können, ist es wichtig, den weiteren Ausbau so effizient und effektiv wie möglich zu gestalten. Kooperationen beim Ausbau können, dort wo sie möglich und sinnvoll sind, einen Beitrag hierzu leisten. Um dies zu ermöglichen müssen

- Informationen zu bestehenden Infrastrukturen möglichst aktuell zur Verfügung stehen. Eine effektive Planung und der Ausbau von TK-Netzen beruhen auf der Kenntnis des Standes zum Zeitpunkt der Planung. Neue Informationen zur Infrastruktur müssen im Idealfall in nahezu Echtzeit verfügbar gemacht werden.
- Die Informationen mit Blick auf die Beurteilung von Kooperationsmöglichkeiten alle relevanten Informationen wie Form (gefördert, eigenwirtschaftlich, kooperativ) und Art (Leerrohr, LWL) vollständig und in einheitlicher Form enthalten. Nur so können Investitionen gezielt und wirtschaftlicher getätigt werden.
- Daten in einheitlichen Formaten verfügbar gemacht werden. Die Informationen aller Infrastrukturbetreiber müssen einheitlich und digital verarbeitbar sein. Nur so kann sichergestellt werden, dass alle am Ausbau mitwirkenden Akteure optimal kooperieren können.

Der Infrastrukturatlas soll eine Grundlage für schnelleren und effizienteren Ausbau von Glasfaser- und Mobilfunknetzen sein. Um dies zu gewährleisten, müssen Datenaktualität, Datenintegrität und Datenqualität optimiert werden.

2.3. Automatisierung und Transparenz

Mit den Neuerungen für das Gigabit-Grundbuch, wurden bereits einige Schritte gegangen, die eine stärkere Transparenz herbeiführen sollen. Aus Sicht des BREKO und dessen Mitglieder lassen diese Schritte jedoch das gestiegene Resilienzbedürfnis der im Infrastrukturatlas aufgeführten Daten außer Acht. Durch eine Automatisierung und Digitalisierung der Prozesse und Standardisierung der Informationen kann nicht nur eine schnelle und transparente Koordinierung ermöglicht werden, sondern auch dem gestiegenen Resilienzbedürfnis Rechnung getragen werden, indem eine Transparenz über die Nutzung der Daten gegenüber der Dateninhabenden Person geschaffen wird.

- Standardisierung: Standardisierte Informationen zu Infrastruktur bzgl. Lokation auf Basis georeferenzierter Daten und in einer Detaillierung, die einerseits zur Bewertung von Ausbauplänen gereicht, erleichtern den Verwaltungsaufwand bei allen Akteuren des Telekommunikationsnetzausbaus.
- Digitalisierung der Datenerfassung: Durch eine Digitalisierung der mit dem ISA verbundenen Prozesse zur Erfassung von Daten erhöht sich die Frequenz der Aktualisierungen von Infrastrukturdaten und damit die Effizienz der Planung. Darüber hinaus wird eine maximale Transparenz über die vorhandene und geplante Infrastruktur geschaffen.

- Digitalisierung der Datenbereitstellung: Die Prozesse zur Beantragung der Einsichtnahme, angefangen bei der Registrierung von Unternehmen und Nutzenden bis zur Antragstellung und Information der Betreibenden müssen maximal digitalisiert und automatisiert werden. Dadurch wird die Beantragung für die Einsichtnahme Beantragenden nicht nur schneller und effizienter. Auf Basis dieser Neuerungen kann auch den Bereitstellern von Daten automatisch eine umfassende Transparenz darüber verschafft werden, von wem und wo Einsichtnahme beantragt wurde.

3. Die Nutzungsgruppen und ihre Anforderungen

Die oben aufgeführten Gründe für einen sicheren, aktuellen und digitalen ISA basieren einerseits auf grundsätzlichen Anforderungen aus Regelungen wie TKG, GIA, KRITIS-DachG, NIS2-Umsetzungsgesetz und anderen. Andererseits existieren aber Anforderungen und Bedarfe der Nutzenden des ISA, die es zu berücksichtigen gilt.

Die Nutzenden des ISA lassen sich in vier wesentliche Gruppen aufteilen, die im Folgenden beschrieben sind. Es sei hier darauf hingewiesen, dass ein Akteur auch mehreren Gruppen angehören kann, d. h. ein Unternehmen kann z. B. sowohl Eigentümer und Betreiber (1) als auch ausbauendes Unternehmen (2) sein.

1. **Eigentümer und Betreiber von Versorgungsinfrastrukturen:** Dazu gehören Telekommunikationsunternehmen, Netzbetreiber sowie Versorgungsnetzbetreiber, die ihre Infrastrukturdaten, wie Leerrohre- und Breitbandnetzstandorte, an den ISA melden. Diese Gruppe spielt eine zentrale Rolle, da sie die erforderlichen Daten für den ISA bereitstellt. Die Meldung der Daten erfolgt aufgrund von Verpflichtungen aber auch aus vertrieblichem Interesse.
2. **Staatliche und kommunale Akteure:** Diese Gruppe umfasst verschiedene Ebenen der öffentlichen Verwaltung, darunter Bund, Länder, Kreise und Kommunen. Sie nutzen den ISA für Planungs- und Koordinationszwecke im Rahmen des Glasfaser- und Mobilfunkausbaus und anderer infrastruktureller Projekte.
3. **Unternehmen und Akteure, die sich am Ausbau von Infrastrukturnetzen beteiligen:** Hierzu zählen Unternehmen, die in den Bau oder die Erweiterung von Infrastrukturnetzen involviert sind, sowie Bauunternehmen, die für die physische Umsetzung der Infrastrukturprojekte zuständig sind. Diese Gruppe nutzt den ISA, um Informationen über bestehende Infrastrukturen zu erhalten und die Grobplanung ihrer Projekte damit unter Berücksichtigung vorhandener Infrastrukturen umzusetzen.
4. **Sonstige Behörden:** Hierzu zählen Institutionen der Legislative und Exekutive

Innerhalb des Bereichs des Glasfaser- und Mobilfunkausbaus verfolgen die verschiedenen Nutzungsgruppen unterschiedliche Ziele und haben damit auch unterschiedliche, und zum Teil konträre Anforderungen. Diese werden im Folgenden aufgeführt. Dabei wurde versucht, die Anforderungen insofern zu harmonisieren, dass diejenigen der einen Gruppe nicht in Widerspruch zu solchen anderer Gruppen stehen.

3.1. Eigentümer und Betreiber von Infrastrukturen:

Die wesentlichen Anforderungen dieser Gruppe an einen optimierten ISA sind:

- Ein der Kritikalität der Infrastruktur angemessener, systematischer Schutz der Informationen gegen Missbrauch und unberechtigte Einsichtnahme und Nutzung
- Minimierung des Risikos vor Angriffen und Sabotage gegen die Infrastruktur
- Begrenzung der herauszugebenden Infrastrukturdaten auf den konkreten Einsichtnahmefall.
- Keine dauerhafte zentrale Speicherung aller vorhanden Infrastrukturen deutschlandweit

- Zwingender Nachweis der Einsichtnahmeberechtigung durch Dokumentation eines Vorhabens oder Projektes
- Transparenz über die Nutzung der eigenen Infrastrukturdaten
- Kenntnis über Einsichtnahmebeantragung und Einsichtnahme inkl. der Auftraggeber bei Dienstleistern
- Verbesserte Funktionalität für die Bereitstellung der meldepflichtigen Daten (Upload-Verfahren)
- Kenntnis über die Einsichtnahme durch sonstige Beteiligte
- Unterstützung unterschiedlicher, aber bestimmter Formate für die Bereitstellung von Daten

3.2. Staatliche und kommunale Akteure

Die Anforderungen dieser Nutzergruppe sind:

- Möglichst hohe Aktualität und angemessene Detailtiefe der Infrastrukturdaten für Analyse- und Steuerungszwecke

3.3. Unternehmen und Akteure, die sich am Ausbau von Infrastrukturnetzen beteiligen

Die Forderungen dieser Gruppe beziehen sich auf:

- Deutlich höhere Aktualität der Infrastrukturdaten
- Schnelle Bearbeitung von Einsichtnahme-Anträgen inkl. der Definition und automatisierter Überwachung der Einhaltung von Fristen für Prozesse (z. B. Prüfung der Berechtigung zur Einsichtnahme)
- Verpflichtung aller Beteiligten zur zeitnahen Bereitstellung der Daten
- Höhere Transparenz der Informationen bzgl. der Ausbauart (gefördert, teil-gefördert, eigenwirtschaftlich) der Infrastruktur
- Höhere Konsistenz der Daten, d. h. einheitliche und anlassbezogene Detailtiefe
- Die Daten sollten in einem einheitlichen Format bereitgestellt werden (dies bezieht sich im Wesentlichen auf den Download bzw. bilateralen Datenaustausch)
- Klar definierte, anlassbezogene und umfassende Pflichtangaben bzgl. der Daten

4. Konzept dezentraler Infrastrukturatlas

Um den oben genannten Anforderungen zukünftig gerecht zu werden, wurde ein Konzept entworfen, welches den folgenden Architektur-Paradigmen folgt:

- Security-by-Design, also die Erreichung eines hohen Sicherheitsstandards durch das Architektur-Design
- Automation-by-Digitalization, also eine hohe Automatisierung der Prozesse durch Nutzung digitaler Technologien

Wesentliches Merkmal ist eine Dezentralisierung der Datenhaltung des Infrastrukturatlas. Im Folgenden wird dieser als dISA (dezentraler Infrastrukturatlas) bezeichnet. Weitere wichtige Merkmale sind:

- Standardisierung der bereitgestellten Daten in Form von georeferenzierten Informationen
- Eine reduzierte Genauigkeit der Daten, die einerseits die Planung unterstützt, andererseits Missbrauch verhindert

- Automatisierung und Digitalisierung der Prozesse
- Erhöhung der Informationssicherheit durch Verschlüsselung aller Daten und erweiterte Authentifizierungsmechanismen

Dieses Konzept ist als Erweiterung und Verbesserung des bereits bestehenden ISA zu verstehen. Im Folgenden werden sowohl die architektonischen Erweiterungen als auch die damit einhergehenden veränderten Prozesse beschrieben.

4.1. Architektur-Konzept

Der dISA setzt sich aus zwei wesentlichen Komponenten zusammen: einerseits einem zentralen, web-basierten dISA-Portal und andererseits den dezentralen Infrastruktur-Datenbanken – dISA-DB. Abbildung 2: Architektur des dezentralen Infrastrukturatlas (dISA) zeigt die Architektur schematisch.

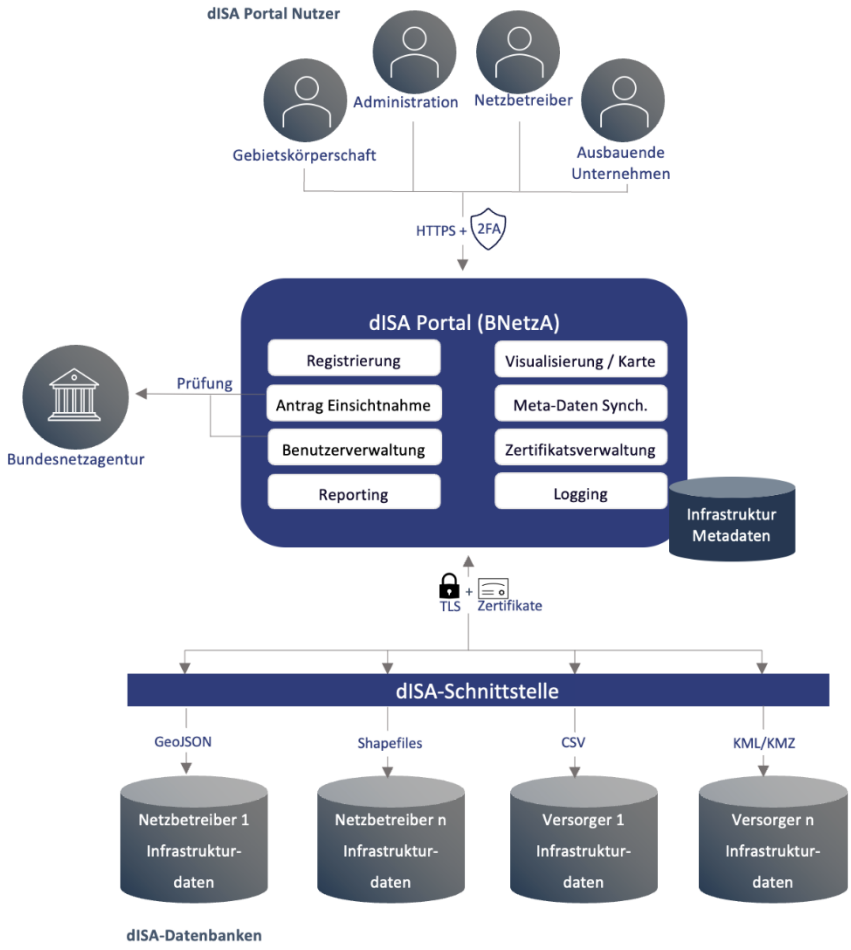

Abbildung 2: Architektur des dezentralen Infrastrukturatlas (dISA)

4.1.1. Funktionale Bausteine

Das dISA-Portal, welches auch als Erweiterung des Gigabit-Grundbuch-Portals realisiert werden könnte, wird durch die Bundesnetzagentur (BNetzA) betrieben. Es stellt die Kommunikationsschnittstelle für alle dISA-Nutzende dar und enthält Meta-Informationen zu den Infrastrukturdaten. Im Wesentlichen sind dies die Zuordnungen von Infrastruktur-Besitzern zu geographischen Daten. Im Portal sind alle Prozesse der verschiedenen Nutzungsgruppen abgebildet. Hierzu gehören

- der Registrierungsprozess inkl. der Prüfung und Bewilligung durch die BNetzA
- Die Prüfung von Anträgen zur Einsichtnahme in bestimmte Infrastrukturen durch die BNetzA inkl. der Entscheidung über die einzusehenden Attribute
- eine kontinuierliche Synchronisation der Meta-Infrastrukturdaten
- die Beantragung der Einsichtnahme inkl. der Benachrichtigung der Infrastruktur-Eigentümer

Eine detaillierte Beschreibung der Prozesse findet sich im nachfolgenden Abschnitt. Weitere funktionale Bausteine des dISA sind:

- intelligente und sichere Nutzendenverwaltung
- Visualisierung der Infrastrukturdaten in Kartenansichten
- Filterung unterschiedlicher Infrastruktur-Objekte
- Ansicht von Detailinformationen zur Infrastruktur
- Zertifikatsverwaltung für sichere und verschlüsselte Kommunikation
- Logging aller Transaktionen zur detaillierten Nachverfolgung von Anfragen
- Ausführliche Reporting-Funktionalität zur Schaffung von Transparenz für alle Nutzende

4.1.2. Metadaten

Metadaten werden zentral in der dISA-Datenbank gespeichert. Die Metadaten enthalten keinerlei Infrastrukturinformationen, sondern stellen nur die Referenz zwischen einer Geolokation und den Infrastrukturbetreibern dar, die an dieser Geolokation Infrastrukturdaten besitzen bzw. betreiben. Grundlage der Geolokationen sind standardisierte Polygone. Einziges Ziel der Metadaten ist, die fallbezogene Abfrage von georeferenzierten Infrastrukturinformationen effizienter zu gestalten, da nur die Infrastrukturbetreiber abgefragt werden, die in einem Polygon auch Infrastrukturen vorhalten.

4.1.3. Georeferenzierte Infrastrukturdaten

Das Konzept des dISA sieht vor, dass die eigentlichen Infrastrukturdaten in den Datenbanken (dISA-DB) der Infrastrukturbetreiber (Nutzungsgruppe 1) verbleiben und im Falle einer positiv beschiedenen Anfrage in nahezu Echtzeit aus diesen Datenbanken im Sinne eines Pull-Prozesses abgefragt werden.

Georeferenzierte Daten bieten die Möglichkeit einer effizienten Verarbeitung in der Planung neuer Infrastruktur. Um aber den Sicherheitsanforderungen an den dISA gerecht zu werden, wird die Genauigkeit der Daten beim Abruf reduziert. Damit bleibt der Nutzen für Planung und Kooperation erhalten, die Risiken durch Missbrauch werden aber reduziert.

Die Kommunikation zwischen dem dISA-Portal und den einzelnen meldepflichtigen Einrichtungen wird mittels der dISA-Schnittstelle realisiert. Für den effizienten Datenaustausch ist es empfehlenswert, dass die verwendeten GIS-Datenformate etablierten Standards entsprechen und konsistent von allen beteiligten Einrichtungen genutzt werden. Um die Betreiber in diesem Prozess zu entlasten, ist die Implementierung mehrerer Datenformate vorgesehen. Mögliche Formate, die in Betracht gezogen werden können, umfassen:

- Shapefiles
- GeoJSON
- CSV inkl. Geokoordinaten
- KML/KMZ
- DWG

- GDB

Die georeferenzierten Daten müssen auch inhaltlich einem gewissen Standard genügen. Die Details des Informationsumfangs können später festgelegt und sukzessive angepasst werden. Grundsätzlich sollten Informationen wie Art des Ausbaus (eigenwirtschaftlich, gefördert), Zeitinformationen zu Ausbau/Planung, Leerrohr oder Glasfaser, vorhanden sein, damit der potenzielle Interessent den Kontakt zum Eigentümer oder Betreiber der Infrastruktur aufnehmen kann (Match-Making). Bei der Beantragung einer Einsichtnahme ist zu spezifizieren, welche Informationen angefordert werden.

4.1.4. Sicherheit des dISA

Um den Sicherheitsanforderungen der unterschiedlichen Nutzungsgruppen aber auch grundlegender Vorgaben (KRITIS-Dachgesetz, NIS2-Umsetztungs- und Cybersicherheitsstärkungsgesetz) gerecht zu werden, sind im Konzept zwei wesentliche Maßnahmen vorgesehen.

Um Zugang zum dISA-Portal zu erhalten, ist für die Nutzenden neben der Authentifizierung mittels Benutzername und Passwort, die verschlüsselt über HTTPS übertragen werden, auch die Verwendung einer Zwei-Faktor-Authentifizierung4 erforderlich. Diese Maßnahme führt nicht nur zu einer zusätzlichen Sicherheitsebene, sondern ermöglicht auch eine präzise Zuweisung der Nutzerkonten zu individuellen Personen. Die Nutzung eines Accounts durch mehrere Mitarbeitende eines Unternehmens ist nahezu unmöglich.

Die Kommunikation zwischen dem dISA-Portal und den einzelnen meldepflichtigen Infrastrukturbetreibern wird mittels der dISA-Schnittstelle realisiert. Für die Authentifizierung der beteiligten Kommunikationsparteien kommt TLS[5] 1.3 oder höher zum Einsatz oder gegebenenfalls mTLS[6]. Nachdem die Authentifizierung erfolgreich abgeschlossen ist, erfolgt der Datenaustausch, welcher durch TLS-Verschlüsselung gesichert ist.

Zur Ermittlung der betroffenen Infrastrukturbetreiber pflegt das dISA-Portal eine Netzbetreiber Metadaten Datenbank. In dieser sind zu allen registrierten Betreibern Polygone hinterlegt, welche Gebiete kennzeichnen, in denen Betreiber Infrastruktur besitzen. Bei einer Einsichtnahmeanfrage werden diese Polygone mit dem angefragten Gebiet abgeglichen, um alle dort vertretenen Infrastrukturbetreiber zu ermitteln. Es ist zu beachten, dass die dISA-Portal-Datenbank keinerlei Daten über konkrete Infrastruktur besitzt. Wie die Infrastrukturdaten zu einer Einsichtnahmeanfrage bereitgestellt werden, ist in 4.2.3 beschrieben.

Im Zuge des Abrufs der georeferenzierten Daten wird deren geographische Genauigkeit durch einen Algorithmus derart reduziert (siehe Kapitel 4.2.5), dass sie für die Ausbauplanung ausreichend ist, aber einen relevanten Schutz gegen Missbrauch darstellt. Unter dieser Prämisse sieht der BREKO es als vertretbar an, einem Download solcher „unscharfen“ Daten zuzustimmen.

Unabhängig davon bleiben die Richtlinien des ISA bzgl. der Nutzung, Verbreitung und Löschung von heruntergeladenen Daten weiterhin bestehen (Einsichtnahmebedingungen für den Infrastrukturatlas der Zentralen Informationsstelle des Bundes (ISA-Planung (Teil 1) und ISA-Mitnutzung (Teil 2)). Jene Einsichtnahmebedingungen regeln auch die Möglichkeiten der BNetzA und der betroffenen Infrastrukturinhaber im Falle eines Verstoßes gegen die Einsichtnahmebedingungen gegebenenfalls Maßnahmen umzusetzen.

[4] Die Zwei-Faktor-Authentifizierung ist ein Sicherheitsverfahren, das zwei verschiedene Identitätsnachweise (wie Passwort und Smartphone-Code) zur Anmeldung verlangt, um höhere Sicherheit zu gewährleisten

[5] TLS (Transport Layer Security) ist ein Protokoll zur Verschlüsselung von Internetkommunikation, das die Sicherheit und Integrität von Daten zwischen Webservern und Clients gewährleistet.

[6] mTLS (Mutual Transport Layer Security) ist eine erweiterte Version von TLS, bei der sowohl der Client als auch der Server ihre Identität mittels Zertifikate verifizieren, um eine sichere bidirektionale Kommunikation zu ermöglichen.

4.2. Prozesse

Im Folgenden werden die wesentlichen Prozesse, die der dISA zur Verfügung stellt, beschrieben. Grundsätzlich werden diese Prozesse durch im dISA implementierte Workflows unterstützt und gesteuert. Dies bedeutet, dass Abläufe strukturiert erfolgen, dass für alle Prozesse die zeitlichen Abläufe in Form von Fristen und deren Überwachung hinterlegt sind und bei Abweichungen entsprechende Benachrichtigungen und Eskalationen erfolgen.

4.2.1. Registrierung/Anmeldung

Auf dem dISA-Portal registrieren sich meldepflichtige Organisationen und Berechtigte zur Einsichtnahme. Die initiale Registrierung einer Organisation unterliegt einer sorgfältigen Überprüfung durch die Bundesnetzagentur. Mit dieser Registrierung wird ein Administrator der Organisation registriert. Dieser kann dann eine begrenzte Anzahl weiterer Nutzender seiner Organisation hinzufügen. Für den Registrierungsprozess stellt das dISA-Portal einen Dialog zur Verfügung. Bei der Erstellung eines neuen Kontos gelten strenge Richtlinien für die Passwortvergabe. Zusätzlich ist die Einrichtung einer Zwei-Faktor-Authentifizierung verpflichtend.

Dazu muss sich die nutzende Person eine Authenticator App (z.B. Google Authenticator, Microsoft Authenticator) auf seinem Smartphone installieren und mit dem dISA-Portal über einen generierten QR-Code verbinden. Diese zusätzliche Sicherheitsebene erfordert bei jeder Anmeldung auf dem dISA-Portal neben den Anmeldeinformationen auch die Eingabe eines zeitlich begrenzt gültigen Einmal-Passworts. Dies ermöglicht eine eindeutige Zuordnung jeder Anmeldung zu einer natürlichen Person und minimiert das Risiko einer Kompromittierung des Benutzerkontos. Zudem werden bei einer Anmeldung die Anmeldeinformationen mit HTTPS verschlüsselt, um ein Auslesen zu verhindern.

Im dISA-Portal verfügen die Nutzenden entsprechend ihrer Rolle über unterschiedliche Ansichten. Einsichtnehmende können über ein Formular Anfragen zur Einsichtnahme eines bestimmten Gebiets stellen und haben die Möglichkeiten zu ihren Anfragen Informationen einzusehen, wie beispielsweise den Status der Anfrage. Im Zuge der Entscheidung über die Genehmigung der Einsichtnahme wird durch die BNetzA festgelegt, welche Informationen dem Antragsteller zur Verfügung gestellt werden. Die Bewilligung einer Einsichtnahme gilt für eine gewisse Dauer. Eine Verlängerung dieser Frist innerhalb einer Zeit von sechs Monaten erfolgt in einem vereinfachten, digitalen Verfahren. Innerhalb der Einsichtnahmefrist erhält der Einsichtnehmende auch Zugang zu innerhalb der Frist aktualisierten Daten.

Datenliefernde Unternehmen erhalten unter anderem eine Reporting-Funktion, die es ihnen ermöglicht, detaillierte Informationen zu Anfragen zu erhalten. Diese Übersicht beinhaltet Informationen darüber, wer Anfragen ihre Daten betreffend gestellt hat, innerhalb welcher Zeiträume Einsicht in ihre Infrastrukturdaten gewährt wurde und aus welchen Gründen diese Anfrage erfolgte. Dadurch wird eine erhöhte Transparenz geschaffen, da besser nachvollzogen werden kann, an wen welche Daten gegeben wurden.

4.2.2. Erstellung und Aktualisierung der Metadaten

Der Upload von flächendeckenden Infrastrukturdaten wie er aktuell im ISA umgesetzt ist, wird durch einen deutlich reduzierten, automatisierten Prozess ersetzt, welcher zu definierten Zeiten in einer ca. wöchentlichen Frequenz ausgeführt wird. Dieser Prozess aktualisiert die Metadaten des dISA-Portals.

Bei Ausführung des Prozesses fragt das dISA-Portal, über die dISA-Schnittstelle, bei allen registrierten datenliefernde Unternehmen nach Polygonen mit neuer Infrastruktur. Die Authentifizierung und Autorisierung der Kommunikationsteilnehmer (dISA-Portal und verteilte dISA-DB) erfolgt zertifikatsbasiert durch TLS in Kombination mit digitalen Signaturen oder auch mTLS. Hierdurch werden betrügerische, nichtautorisierte Abfragen (z. B. Hacker-Angriffe) verhindert. Der Transport der Infrastrukturdaten erfolgt verschlüsselt auf Basis von TLS, wodurch ein Mitlesen oder Mitschneiden des Datentransfers verhindert wird.

Im Zuge des Datentransfers wird eine Konsistenz- und Vollständigkeitsprüfung der Daten durchgeführt. Werden hier Abweichungen von den Anforderungen und Standards festgestellt, werden die datenliefernde Unternehmen hierüber informiert und zur Behebung aufgefordert. Die BNetzA wird ebenfalls über den Status informiert. Auf Basis der gelieferten und korrekten Daten werden die Metadaten neu gebauter Infrastruktur berechnet und in der Metadaten-Datenbank abgelegt bzw. bestehende Informationen aktualisiert. Die Infrastrukturdaten werden nicht gespeichert und nach der Prozessierung umgehend automatisch gelöscht.

4.2.3. Einsichtnahme

Berechtigte Nutzende müssen für die Einsichtnahme einen Antrag über ein Formular im dISA-Portal stellen. Für die Auswahl des Gebietes gibt es die Option, ein Polygon auf einer Karte einzuzeichnen oder das Polygon in Form einer Datei hochzuladen. Für staatliche und kommunale Akteure (Gruppe 3) können weitergehende Abfragekriterien implementiert werden. Informationen zu Kontaktpersonen, zum Projekt oder Vorhaben (inklusive eines Nachweises in Form einer Vorhabenbeschreibung) müssen angegeben werden. Die BNetzA prüft die Anfrage anhand eines transparent einsehbaren Prozesses. In diesem werden den prüfenden Mitarbeitenden anhand der Metadaten und des angefragten Gebiets alle Informationen zur Beurteilung der Anfrage bereitgestellt. Auf Basis der Metadaten werden die Infrastrukturbetreiber, die im ausgewählten Gebiet Infrastruktur besitzen, ermittelt. Bei positiver Entscheidung des Antrages startet dann der Prozess der Datensammlung wie in Kapitel 4.2.4 beschrieben.

Des Weiteren wird der Antragsteller automatisch über die Entscheidung informiert, dasselbe geschieht auch bei einer negativen Entscheidung. Die Infrastrukturbetreiber, von welchen auf Grund des Einsichtnahmeantrags Daten abgefragt werden, werden ebenfalls über die Anfragenden und Polygondaten informiert.

Für die datenliefernden Unternehmen gibt es verpflichtende Anforderungen an Güte und Umfang der freigegebenen Infrastrukturdaten bezüglich genauer Angaben von Attributen wie z. B. gefördert/eigenwirtschaftlich/kooperativ, Leerrohr/LWL.

Der gesamte Prozess der Einsichtnahme und der Datenlieferung wird im dISA-Portal protokolliert und gespeichert, sodass zu jeder Zeit nachvollziehbar bleibt, wer welche Informationen erhalten hat.

4.2.4. Datenbereitstellung bei Einsichtnahme

Nach bewilligtem Antrag zur Einsichtnahme und Abruf der Daten durch den Einsichtnehmenden bezieht das dISA-Portal mittels Pull-Verfahren[7] die Daten aus den jeweiligen dISA-Datenbanken der für die Abfrage relevanten Infrastrukturbetreibern in das dISA-Portal. Grundlage für die transferierten Daten sind die Polygone der Anfrage. Im Zuge des Transfers werden die Daten einer automatischen Datenkonsistenzprüfung unterzogen, in ein einheitliches Format transferiert sowie durch das in Kapitel 4.1.4 beschriebene Verfahren in der Genauigkeit reduziert.

Sollten die erhaltenen Infrastrukturdaten oder ihre jeweiligen Attribute unzureichend sein, wird das datenliefernde Unternehmen darüber informiert und aufgefordert die Inkonsistenzen zu beheben. Erfüllen die Daten die Anforderungen, werden sie dem Antragsteller im dISA zeitlich begrenzt zur Einsichtnahme und zum Download zur Verfügung gestellt.

In diesem Zuge findet keine Speicherung der erhaltenen Daten im dISA-Portal statt, da diese aus Sicherheitsgründen dezentral bei ihren Eigentümern verbleiben. Während der Einsichtsperiode kann über das dISA-Portal eine Aktualisierung der Infrastrukturdaten oder eine Verlängerung der Frist beantragt werden. Mit Ablauf der Frist sind die zuvor freigegebenen Daten nicht mehr zugänglich und

[7] Beim Pull-Verfahren stellt eine anfragende Seite einer Datenkommunikation einen Abruf von Daten an eine liefernde Seite, im Gegensatz zum Push-Verfahren.

ein neuer Antrag muss gestellt werden. Der vollständige Datentransport erfolgt verschlüsselt und signiert auf Basis von TLS oder mTLS.

4.2.5. Bereitstellung von georeferenzierten Daten zur Verarbeitung in GIS-Systemen

Eine wesentliche Frage ist, wie man den hohen Anforderungen an die Informationssicherheit bzgl. der Infrastrukturdaten einerseits und dem Bedarf an einer effizienten Nutzung der Daten im Rahmen der Planung und des Baus von Gigabit-Infrastrukturen andererseits gerecht werden kann.

Ein Download von detaillierten georeferenzierten Infrastrukturdaten aus dem dISA scheint unter Sicherheitsaspekten nicht akzeptabel. Ohne eine Bereitstellung von digitalen Daten wird aber kein echter Mehrwert für die Ausbauplanung geschaffen. Aus diesem Grund wurde ein Weg gewählt, der beiden Aspekten gerecht wird. Die Daten werden in ihrer Genauigkeit soweit reduziert, dass ein Missbrauch, im Sinne von Kompromittierung von Infrastruktur, deutlich erschwert ist. Der Nutzen dieser Daten für die Planung ausbauender Unternehmen aber bleibt erhalten und eines der Ziele des dISA, eine Vermittlung zwischen Infrastrukturbetreibern und ausbauenden Unternehmen, die ein Interesse an Mitnutzung von Infrastruktur haben, ist gewährleistet. Grundlegende Angaben, wie die Streckenlänge sowie die Lage von verlegter Infrastruktur zu Georeferenzpunkten (wie Flüsse, Autobahnen oder Bahnstrecken) werden in der Art abgebildet sein, dass klar hervorgeht, auf welcher Seite der Georeferenzpunkte die Trassen verlaufen, um Querungen zu vermeiden. Damit ist ein Download von georeferenzierten Daten aus dem dISA vertretbar.

5. Maßnahmen zur Realisierung

In diesem Kapitel werden in einer ersten Annäherung die notwendigen technologischen Maßnahmen zur Realisierung des dISA dargestellt. Eine detaillierte Spezifikation ist Teil von nachfolgenden Aktivitäten. Die technologischen Maßnahmen lassen sich in drei Gruppen aufteilen

1. Maßnahmen auf Seiten der zentralen dISA-Plattform, also der BNetzA
2. Maßnahmen auf Seiten der Eigentümer und Betreiber von Versorgungsnetzen (Nutzungsgruppe 1) und damit der datenliefernden Unternehmen
3. Maßnahmen auf Seiten von Softwareunternehmen für Netzdokumentation, Asset-Management, Network-Inventory, Bauplanung

5.1. Maßnahmen dISA

Für die Umsetzung des dISA müssen folgende Schritte umgesetzt werden:

- Schaffung eines web-basierten Portals
- Erstellung einer Datenbank für die Metadaten
- Implementierung einer Kontoverwaltung
- Implementierung einer Benutzungsoberfläche für die unterschiedlichen Prozesse
- Implementierung der beschriebenen Prozesse als Workflows
- Etablierung einer Zertifikatsverwaltung
- Implementierung von Algorithmen zur Konsistenzprüfung, zur Berechnung der Metadaten, für die Konversion von Geo-Formaten und zur Reduktion der Genauigkeit der Geodaten
- Implementierung der Darstellung von Daten in einer Kartenansicht
- Implementierung einer Schnittstelle, die von datenliefernden Unternehmen bzw. SW-Herstellende als Gegenseite des Pull-Prozesses integriert werden kann
- Implementierung eines umfassenden Loggings und Reportings

5.2. Maßnahmen Infrastrukturbetreiber

Mit der Umsetzung eines dISA müssen Infrastrukturbetreiber

- Infrastrukturdaten in den vorgesehenen Formaten sowie mit den geforderten Attributen aktuell vorhalten
- Soweit eigene Software genutzt wird, die bereitgestellte Schnittstelle integrieren
- Ein Zertifikat für die Authentifizierung generieren

5.3. Maßnahmen von Softwareunternehmen

Softwareunternehmen für Applikationen zur Verwaltung von Netzinfrastruktur können ihre Tools

- mit einer entsprechenden Schnittstelle ausstatten
- um die definierten Datenformate und Attribute erweitern, soweit erforderlich
- und die notwendigen Komponenten für sichere Kommunikation implementieren

6. Fazit

Mit dem vorgestellten Konzept des dISA werden wesentliche Forderungen sowohl der am Infrastrukturausbau beteiligten Unternehmen und Organisationen als auch grundsätzliche Anforderungen an Kritische Infrastruktur erfüllt.

Durch die Dezentralisierung wird ein deutlich höheres Sicherheitsniveau erreicht, ein Angriff auf das zentrale dISA-Portal richtet nur marginalen Schaden an, da dort keine relevanten Infrastrukturdaten gespeichert werden. Diese Maßnahme deckt Forderungen, die sich aus KRITIS-DachG und NIS2-Umsetzungsgesetz ergeben, ab.

Hierauf zahlt auch die vollständige Verschlüsselung des Datentransports ein.

Die Einführung einer Zwei-Faktor-Authentifizierung verhindert die Weitergabe von Login-Daten, und damit den Kontrollverlust des Zugangs zum dISA.

Mit den oben genannten Maßnahmen ist auch eine exakte Nachverfolgbarkeit (Logging) aller Aktivitäten möglich, was sowohl im Sinne der Auditierung ist als auch der Erkennung und Verfolgung von unlauterem Wettbewerb dienlich ist.

Auf Basis der Logging-Daten und des Reportings erhalten alle Beteiligten detaillierte Einsichten bzgl. der ihre Daten betreffenden Aktivitäten und Transaktionen, was den Anforderungen nach Transparenz und Nachvollziehbarkeit nachkommt.

Die Automatisierung aller Prozesse zahlt auf die Effizienz und Bearbeitungsdauer von Abläufen ein. Vorgänge werden einer zeitlichen Kontrolle unterworfen und beim Erreichen oder Überschreiten von zeitlichen Vorgaben werden Eskalationen gestartet. Dies entspricht den Forderungen nach schnellerer Bearbeitung und Beantwortung von Anfragen, sowohl bei der Registrierung als auch bei Einsichtnahme-Anfragen.

Nicht zuletzt wird durch das Gesamtkonzept der dezentralen Datenhaltung und automatisierten, regelmäßigen Aktualisierung der Daten der Forderung nach Aktualität nachgekommen. Dazu kommt eine höhere Qualität der Daten durch definierte Standards.

Mit dem vorliegenden Konzept eines dezentralen Infrastrukturatlas wird ein wesentlicher Schritt im Sinne einer sicheren Digitalisierung gegangen, mit dem den Verpflichtungen bzgl. der Informations- und Datenbereitstellung aus den einschlägigen Regelungen (TKG, GIA, Kostensenkungsrichtlinie für den Breitbandausbau, Europäischer Kodex für elektronische Kommunikation) sowie den Anforderungen an eine hohe Resilienz und Sicherheit (KRITIS-DG, NIS2-Umsetzungsgesetz) Rechnung getragen würde.