

**POSITIONSPAPIER**  
**KOMMUNALER CYBERRAUM**



**Autoren**

Max Schulze-Vorberg  
Dr. Michael Tschichholz

**Mit freundlicher Unterstützung von**

Rolf Prudent  
Karl-Heinz Löper  
Roman Konzack

Fraunhofer-Institut für  
Offene Kommunikationssysteme FOKUS  
Kompetenzzentrum ELAN  
Kaiserin-Augusta-Allee 31  
10589 Berlin

Tel. +49 30 3463-7115  
Fax +49 30 3463-99 7115  
elankontakt@fokus.fraunhofer.de

www.fokus.fraunhofer.de

**Institutsleitung**

Prof. Dr. Dr. h.c. Radu Popescu-Zeletin  
Gerd Schürmann

**Gestaltung, Satz, Bildredaktion**

Dominic Gorny  
Guido Lembeck

**Gesamtherstellung**

LaserLine Druckerei

**Bildnachweis**

Titelgrafik "Old and new 1" (cc) Jan Ramroth, flickr  
S. 5 "Berlin Hauptbahnhof" (cc) onnola, flickr  
S. 11 "old and new 2" (cc) Jan Ramroth, flickr  
S. 13 "Leben im Netz" © Ismanah  
S. 16 "European Commission" (cc) Sébastien Bertrand, flickr  
S. 19 "Steine bilden Weg mit Linie" © Robert Kneschke, fotolia

**DIE INITIATOREN 2****DIGITALE EVOLUTION 4**

Die „digitale Evolution“ verändert das Zusammenwirken von Zivilgesellschaft, Politik und Verwaltung. Damit entstehen neue Herausforderungen und Möglichkeiten für den Standort Deutschland und seine Position im internationalen Wettbewerb.

**KOMMUNEN ALS DREHSCHWEIBEN 6**

Kommunen bilden traditionell die Knotenpunkte zwischen Zivilgesellschaft, Wirtschaft und öffentlicher Verwaltung. Sie entwickeln sich zu „digitalen Dienstleistungszentren“ im öffentlichen Raum.

**KOMMUNALER CYBERRAUM SCHAFFT EFFIZIENZGEWINN 10**

Technologische und organisatorische Voraussetzung sind Kommunale Cyberräume als Kommunikationsplattform. Die nötigen Technologien sind zu großen Teilen bereits vorhanden, sie müssen intelligent integriert und Ergänzungen noch entwickelt werden.

**VERNETZUNG IN KOOPERATIVEN ENTWICKLUNGSVERBÜNDEN 12**

Kommunale Cyberräume sind erfolgskritisch für die Nationale E-Government-Strategie. Organisatorische Voraussetzung ist deshalb die schrittweise Vernetzung in kooperativen Entwicklungsverbänden über die staatlichen und die kommunalen Ebenen hinweg.

**PERSPEKTIVE BRÜSSEL 16**

Kommunale Cyberräume, die die subsidiäre Leistungsfähigkeit der Kommunen stärken, brauchen die Unterstützung von Bund, Ländern und Kommunen in Abstimmung mit relevanten EU-Regelungen.

**INITIATIVE KOMMUNALER CYBERRAUM – HANDLUNGSBEDARF 18**

Fünf Handlungsfelder stehen im Fokus der Initiative: Rahmenbedingungen, Referenzarchitektur, Migrationsstrategien, Umsetzungsszenarien, Kommunikationsmaßnahmen



**Der föderale Dialog für den Kommunalen Cyberraum beginnt jetzt**

Die "Digitale Kommune der Zukunft" lässt sich nur dann verwirklichen, wenn es auch in der virtuellen Welt gelingt, "Vertrauensräume" aufzubauen, mit denen Datenschutz, Verfügbarkeit und Integrität der

Kommunikation zwischen und innerhalb von Verwaltung, Politik und Zivilgesellschaft gesichert sind.

Mit dem Positionspapier "Kommunaler Cyberraum" wollen der Kommune 2.0 e. V. und Fraunhofer FOKUS auf Bundes- und Länderebene das Bewusstsein dafür schärfen, dass dieses Ziel mit vereinten Kräften zu erreichen ist. Den Kommunen als "digitalen öffentlichen Dienstleistungszentren" kommt eine entscheidende Rolle bei der Gestaltung einer „digitalen Daseinsvorsorge“ zu. Zunächst muss die Anschlussfähigkeit an die heterogenen Rahmenbedingungen in den unterschiedlich aufgestellten Bundesländern geschaffen und, wo es nötig ist, Lücken geschlossen werden. Die damit verbundenen organisatorischen, rechtlichen und technischen Herausforderungen können Kommunen jedoch zeitnah und kosteneffizient nur mit der Unterstützung der Länder umsetzen.

Der Kommune 2.0 e. V. setzt sich deshalb für einen Dialog von Kommunen, Ländern und dem Bund ein. Nur, wenn auch der Bedarf von Städten, Kreisen und Gemeinden beachtet wird, können sichere nationale E-Government-Strategien erfolgreich realisiert werden.

Wolfgang Scherer  
Kommune 2.0 e. V.



**Der Kommunale Cyberraum ist Basis für die „Digitale Agenda“**

Stadtplanung, Partizipation und die Bereitstellung von Diensten in allen für das Leben und Wirtschaften in der Stadt wichtigen Politikfeldern, finden im Kommunalen Cyberraum eine sichere Umgebung und Grundlage. Mehr Lebensqualität, Ressour-

censchonung, Nachhaltigkeit und Standortattraktivität in Städten des 21. Jh. ist ohne kommunalen Cyberraum nicht möglich. Er ist zugleich der Analyse-, Strategie- und Werkzeug der Verwaltung und das Gehäuse der Zivilgesellschaft. Es bedarf sicherer und umfangreicher digitaler Infrastrukturen, die auch neue Arbeitsmodelle und -formen von Kleinstunternehmen unterstützen. Der kommunale Cyberraum bildet die Basis für den „Campus Stadt“. Mobilität, Bildung, Gesundheit, Energie und Sicherheit finden darin zu einem Service- und Aktivitätsraum der Bürgergesellschaft zusammen. Kommunale Politik wird gestärkt, Identität und Orientierung vermittelt. Neue integrierte Dienstleistungen sind künftig die Basis einer integrierten Stadt- und Regionalentwicklung.

Es ist Zeit, dass Bund, Länder und Kommunen eine gemeinsame „Digitale Agenda“ aufstellen. Für die Länder bedeutet dies die Rolle als Impulsgeber, Unterstützer und Enabler. Der Deutsche Städte- und Gemeindebund wird den hierfür notwendigen Dialog mit vorantreiben. Die Initiative Kommunaler Cyberraum bietet dazu ein gutes Forum.

Franz-Reinhard Habel  
Deutscher Städte- und Gemeindebund



**Kommunen als maßgebliche Akteure**

Digitalisierung aus Sicht der Kommunen betrifft v.a. Daseinsvorsorgeleistungen, Antragsangelegenheiten, sowie mehr Möglichkeiten der Bürgerbeteiligung. Das gilt für Bildung, Pflege, Gesundheitsvorsorge oder soziale Integration ebenso wie

für Energiewende und mobile Informationssysteme. Städte, Landkreise und Gemeinden möchten für Bürger wie für die Wirtschaft zeitgemäß, d.h. schnell und effizient da sein. Grundvoraussetzungen sind Medienkompetenz – hier kommt den Kommunen eine wichtige Unterstützerfunktion zu – und die digitale Infrastruktur, sprich flächendeckendes Hochleistungsbreitband, gerade im ländlichen Raum. Zudem werden für die rechtssichere, datenschutzkonforme Abwicklung von Verwaltungsverfahren, Räume benötigt, sie Vertraulichkeit, Verfügbarkeit und Integrität der Kommunikation zwischen Bürgern, Wirtschaft sowie der Politik und der Verwaltung sichern. Anstelle eines isolierten Vorgehens der Landkreise und kreisfreien Städte, sollten Bund, Ländern und Kommunen zusammenwirken. In den technisch-organisatorischen Fragen betrifft das v.a. die Abstimmung zwischen Land und Kommune. Für Rahmenvorgaben, Standardisierung, ggfs. Bereitstellung von Basisinfrastrukturen (Netze etc.) ist der Bund zuständig.

Mit den Kommunen als Gestalter und maßgeblichen Akteuren bietet der „Kommunale Cyberraum“ die Chance, Digitalisierung und medienbruchfreie Verwaltung endlich Realität werden zu lassen.

Dr. Kay Ruge  
Deutscher Landkreistag



**Den Perspektivwechsel mit vereinten Kräften gestalten**

Die vom IT-Planungsrat verabschiedete "Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung" setzt bereits wichtige Vorgaben für den Dialog zwischen Bund, Ländern und Kommunen. Sie zielen auf einheitliche Sicherheits-

standards zum Aufbau von sicheren Infrastrukturen für die digitale Daseinsvorsorge.

Mit dem Vorhaben "Kommunaler Cyberraum" soll nun die Brücke zu den Kommunen geschlagen werden. Um Verwaltungsebenen-übergreifende IuK-Infrastrukturen und -Dienste zu erreichen, müssen Politik, Verwaltungsspitze und IT-Dienstleister auf und zwischen allen föderalen Ebenen zusammenarbeiten. Als wissenschaftliche Einrichtung der angewandten F&E bringen wir die Kompetenz für eGovernment-Rahmenarchitekturen ein, die als Grundlage für übergreifende Empfehlungen dienen können, um die erforderliche Interoperabilität flexibel sicherzustellen. Zudem unterstützen wir als Mediator die zielorientierte und effektive Zusammenarbeit der Stakeholder in den einzelnen Aufgabenbereichen. Wir werden konkrete Projekte im Rahmen dieses Vorhabens initiieren und mit Partnern durchführen.

Wir laden mit diesem Positionspapier alle interessierten Partner aus Politik, Verwaltung, Wirtschaft und Wissenschaft ein, sich an diesem ambitionierten Vorhaben zu beteiligen, um gemeinsam die erforderlichen Perspektiv- und Paradigmenwechsel erfolgreich zu gestalten.

Gerd Schürmann  
stellv. Institutsleiter  
Fraunhofer Institut FOKUS



# DIGITALE EVOLUTION

Die „digitale Evolution“ verändert das Zusammenwirken von Zivilgesellschaft, Politik und Verwaltung. Damit entstehen neue Herausforderungen und Möglichkeiten für den Standort Deutschland und seine Position im internationalen Wettbewerb.

## DIE DASEINSVORSORGE WIRD DIGITAL

Die „digitale Evolution“ verändert zunehmend das Zusammenwirken von Zivilgesellschaft, Wirtschaft, Politik und Verwaltung. Öffentliche IuK-Infrastrukturen erfüllen heute bereits Schlüsselfunktionen für die Organisation der Daseinsvorsorge auf staatlicher und kommunaler Ebene. Mit der zunehmenden Verbreitung von intelligenten Internetdiensten stehen neue Services bereit – so zum Beispiel

- für Informationssysteme zur öffentlichen Sicherheit
- für Bildung und Arbeitsmarkt
- für die soziale Integration zur Bewältigung des demografischen Wandels
- für Sozial-, Pflege- und Gesundheitssysteme
- für vernetzte mobile Informationssysteme
- für die effizientere Nutzung von Energieressourcen
- für die nachhaltige Entwicklung von Wirtschaftsstandorten

## MEHR INTERAKTION FÜR DIE DEMOKRATIE

Die digital unterstützte Verwaltung mit ihrem wachsenden Fundus an bürgerorientierten Informationen und Partizipationsmöglichkeiten bildet zugleich auch die Basis für neue Formen einer „digitalen Demokratie“:

- Über Bürgerportale beteiligen sich Bürgerinnen und Bürger an Abstimmungen und Ideenwettbewerben und erarbeiten Vorschläge zur Entwicklung von kommunalen Projekten.
- Mit neuen Formen der Partizipation entstehen zugleich neue Erwartungen an die Transparenz politischer Entscheidungswege.
- Durch mehr Partizipation und Transparenz soll eine nachhaltige Entwicklung zu mehr bürgerschaftlichem Engagement mit Hilfe von Kooperationsportalen gefördert werden.

Vereinbarkeit mit kommunaler Selbstverwaltung



Noch immer wird befürchtet, dass Ebenen-übergreifende Infrastrukturen die kommunale Organisationshoheit unterlaufen.

Im Forschungsprojekt „Stein-Hardenberg 2.0“ wurde aufgezeigt, dass es eine Gestaltungsaufgabe für die Entwicklung Kommunaler Cyberräume ist, die Effizienz- und Effektivitätspotenziale von vernetztem E-Government mit den legitimationsdominanten Zielen von staatsorganisatorischen Prinzipien in Übereinstimmung zu bringen. Konkret bedeutet dies, dass auch kommunale Selbstverwaltung vor dem Hintergrund von E-Government neu auszu-deuten ist. Die bisherige Interpretation stammt aus einer Zeit, in der es Vernetzungsmöglichkeiten mit IuK Technologien noch nicht gab.

Im Projekt wurde deutlich, dass Infrastrukturaufgaben, wie die Bereitstellung von IT-Systemen und Kommunikationsnetzen, als Unterstützungsaufgaben nicht unter die mit der kommunalen Selbstverwaltung verbundene Organisationshoheit fallen. Organisationshoheit kann als Kompositionshoheit neu gedeutet werden, indem Kommunen mit entscheiden über die Zusammenstellung und Art der Nutzung der IuK-Infrastrukturkomponenten.

Das Verständnis kommunaler Selbstverwaltung als ausschließliche Eigenproduktion wird sich durch Möglichkeiten der Vernetzung verändern. Kommunen werden dazu übergehen, Prozessteile und IuK-Infrastrukturkomponenten auszulagern bzw. einzukaufen.

Prof. Dr. Tino Schuppan  
Wissenschaftlicher Direktor  
ifG.CC - The Potsdam Institute for eGovernment

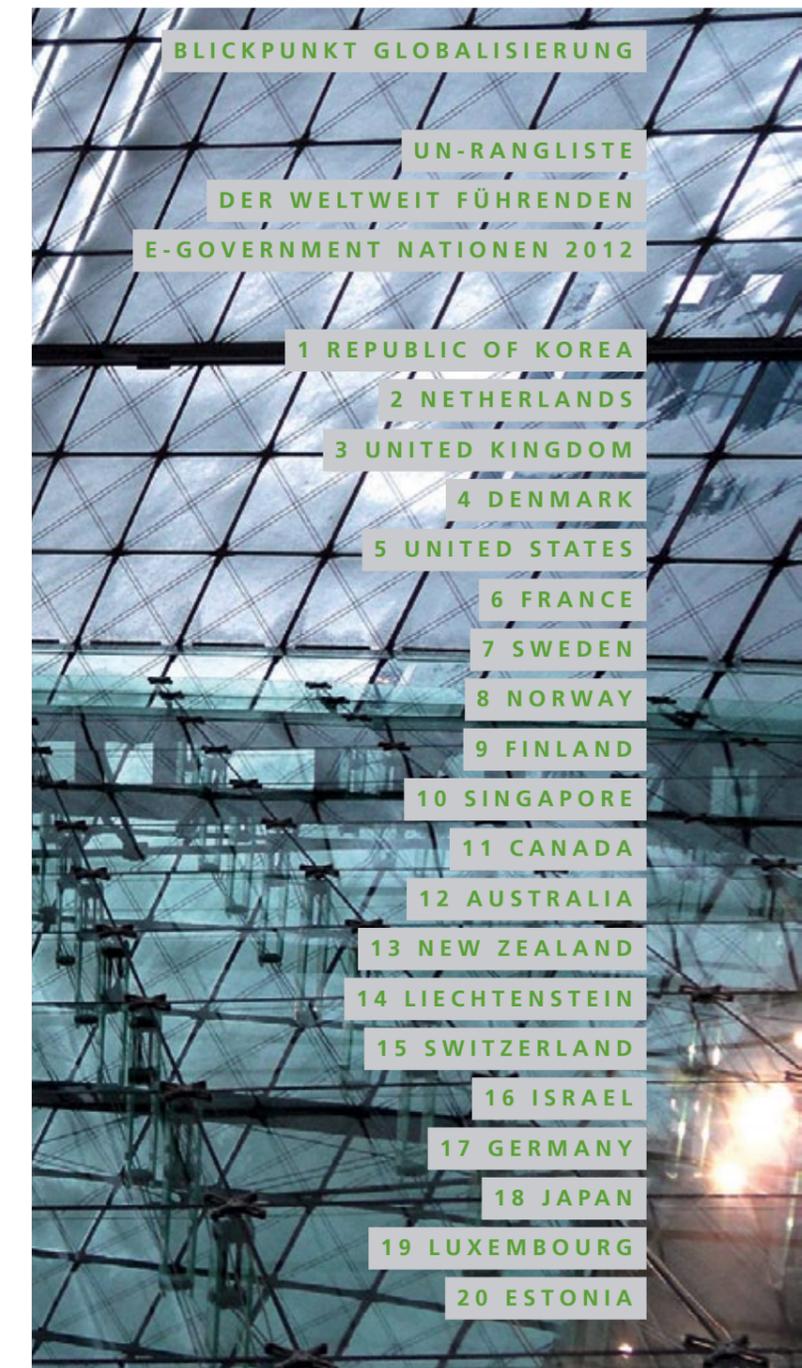
FÜR DEN STANDORT DEUTSCHLAND IST ES ENTSCHEIDEND, DIE SCHLÜSSELFUNKTIONEN DER DASEINSVORSORGE ZU DIGITALISIEREN

## ÖFFENTLICHE VERWALTUNG IM INTERNATIONALEN WETTBEWERB

Im Jahr 2016 werden voraussichtlich drei Milliarden Menschen das Internet nutzen. Der freie Zugang zu Informationen einer digital gestützten Verwaltung wird international unter dem Begriff „Open Government“ diskutiert. In immer mehr Ländern werden neue rechtliche und organisatorische Rahmenbedingungen geschaffen, um die technischen Möglichkeiten für die digitale Daseinsvorsorge zu nutzen. Zu den international aktiven Anbietern neuer Plattformen und Services zählen australische und asiatische Behörden ebenso wie amerikanische und europäische Institutionen. Im internationalen Wettbewerb um die innovative Verwaltung hat die Europäische Union bereits zu Beginn des Jahrzehnts im Aktionsplan 2011–2015 ambitionierte Ziele vorgegeben.

## DEUTSCHLAND HAT AUFHOLBEDARF

Mehr als drei Viertel aller Bundesbürgerinnen und -bürger nutzen heute bereits regelmäßig das Internet. In Bezug zur öffentlichen Verwaltung liegen die Nutzungszahlen gegenüber anderen Ländern allerdings noch zurück. Im internationalen Vergleich konnte die Bundesrepublik Deutschland noch keine Spitzenpositionen einnehmen. In der jüngsten Studie der Vereinten Nationen zur Entwicklung nationaler E-Government-Infrastrukturen aus dem Jahr 2012 lag die Bundesrepublik nur auf Platz 17. Die Gründe dafür sind vielfältig. Sie liegen u. a. in einem fehlenden (politischen) Bewusstsein der Bedeutung dieser Fragen, zu geringen personellen und finanziellen Ressourcen bzw. auch der nicht immer effektiven Steuerung dieser Ressourcen.



# KOMMUNEN ALS DREHSCHWEIBEN

Kommunen bilden traditionell die Knotenpunkte zwischen Zivilgesellschaft, Wirtschaft und öffentlicher Verwaltung. Sie entwickeln sich zu „digitalen Dienstleistungszentren“ im öffentlichen Raum.

## DAS KOMMUNALE HANDELN WIRD TRANSPARENTER

Herausforderungen und Chancen, die mit dem Einzug von sozialen Medien, Bürgerportalen und D115-Services verbunden sind, werden gerade im kommunalen Kontext unmittelbar wirksam. Immer mehr kommunale Politiker und Verwaltungsmitarbeiter bereiten deshalb einen Kulturwandel vor:

Kommunale Behörden verändern sich seit langem von einer geschlossenen, hoheitlich auftretenden Administration hin zu einer kooperativ und transparent agierenden Dienstleistungsorganisation.

Die Zusammenarbeit zwischen Verwaltung, Kommunalparlamenten, Bürgerschaft und Wirtschaft wird heute bereits in vielen Orten leicht verständlich dargestellt durch

- offene Ratsinformationssysteme, mit der sich Bürgerinnen und Bürger über Projekte informieren können, von denen sie unmittelbar betroffen sind,
- integrierte Transaktionsportale für Bürgerschaft und Unternehmen, über welche die grundlegenden Dienste der Verwaltung neben Post, Bürgerbüros, Service D115 auch abschließend über Internet abgewickelt werden können,
- interaktive Informations- und Beteiligungsportale für Stadtplanung und Quartiersmanagement, für Kindertagesstätten, Pflegebörsen und Nachbarschaftshilfen,
- Kooperationsportale für das Vereinsleben zu Bildung, Freizeit, Sport etc.,
- Plattformen für die transparente Vergabe und Abwicklung von öffentlichen Aufträgen zwischen Verwaltung und Wirtschaftsunternehmen.

## KOMMUNALE AKTEURE ENTWICKELN REGIONALE WERTSCHÖPFUNGNETZE

Mit der Unterstützung durch digitale Dienste werden Bürgerinnen und Bürger, Wirtschaftsunternehmen und kommunale Akteure aus dem kulturellen und sozialen Bereich zu aktiven Partnern bei der Bewältigung aktueller politischer Herausforderungen. Digitale Portale und Plattformen von innovativ agierenden Kommunen vereinfachen schon heute die Tätigkeiten von Leistungsträgern und Partnern der kommunalen Verwaltung. Durch Vernetzung wird die kooperative Gestaltung der Daseinsfürsorge in vielen Handlungsfeldern unterstützt:

### Öffentliche Sicherheit

Feuerwehren, THW, Sicherheitsunternehmen, Verkehrsverbände, Versicherungswirtschaft, Wetterdienste, technische Dienstleister etc.

### Soziales

Sozialverbände, Vereine, Kindertagesstätten, Jugendhilfe, Religionsgemeinschaften etc.

### Bildung

Schulen, Hochschulen, IHKs, Handwerkskammern, Wirtschaftsunternehmen, Volkshochschulen etc.

### Arbeitsmarkt

Bundesagentur für Arbeit, regionale Jobcenter, IHKs, Handwerkskammern, regionale Unternehmen etc.

### Energie

Energieversorger, Stadtwerke, Energiegenossenschaften etc.

### Mobilität

Nahverkehrsunternehmen, Bahnunternehmen, Car Sharing, Fernbusunternehmen, Flughäfen etc.



### Gesundheit und Pflege

Krankenhäuser, Pflegeeinrichtungen, Ärzte, Krankenversicherungen, Kliniken, Rotes Kreuz, Johanniter, Volkssolidarität, öffentlicher Gesundheitsdienst etc.

### Kultur

Konzertveranstalter, Museen, Bibliotheken, Theaterorganisationen, Medien- und PR-Unternehmen, Künstler, Bildungseinrichtungen etc.

## OFFENE DATEN UND INTERAKTIVE KOMMUNIKATION DURCH NEUE DIENSTE

In Ergänzung zu den „traditionellen“ Verwaltungsverfahren wird die umfassende Bereitstellung und Nutzung von Daten die Rolle von Kommunen als Leistungszentren für Information und Kommunikation weiter aufwerten. Die Verarbeitung dynamisch erfasster Daten durch verwaltungsinterne oder auch verwaltungsexterne Informationsanbieter

- ermöglicht transparentere regionale Verkehrsinformationen,
- ist Grundlage für aktuelle Warn- und Informationssysteme zur öffentlichen Sicherheit,
- fördert den effizienteren Umgang mit Energieressourcen,
- erleichtert den Zugang zu elektronischen Dienstleistungsangeboten im kommunalen Umfeld,
- bietet neue Services für Pflege und Gesundheit zur Bewältigung des demografischen Wandels,
- setzt Impulse für nachhaltig orientiertes Haushalten,
- schafft mehr Transparenz für politisches Engagement.

### Gesellschaftliche Mehrwerte



Bei der Öffnung hin zu einer dialogbereiten Kommune hat die Bereitstellung offener Daten besondere Bedeutung. Nicht nur neue Nutzungsmöglichkeiten entstehen, sondern auch innovative Impulse für eine partizipative Stadtpolitik sowie neue Räume für kooperative Handlungsmöglichkeiten und -felder. Damit können Brücken über das manchmal sehr ausgeprägte Gegeneinander zwischen Bürgerschaft, Politik und Verwaltung gebaut werden und die vielbeschworene Verantwortungsgemeinschaft neu belebt und schließlich gelebt werden.

Die Kommune als die nächste staatliche Institution für die Bürgerinnen und Bürger ist dabei in besonderem Maße gefordert, sich auf neue Wege und einen eigenen Lernprozess einzulassen, der nicht in jedem Schritt und jeder Konsequenz planbar ist. Die Entwicklung und Gestaltung einer digital unterstützten Kommunikationskultur erfordert Verständnis für unterschiedliche Bedürfnislagen in der Bürgerschaft. Dabei gelten nicht nur die Anforderungen der sogenannten „digital natives“. Unterschiedliche Bevölkerungsgruppen werden lernen, auf neue Weise miteinander umzugehen.

Die Vielfalt der Aufgaben erfordert auch eine neue Qualität der Vernetzung zwischen Kommunen und den anderen staatlichen Ebenen im kommunalen Cyberraum. Erfahrungen anderer Städte, Überlegungen von Bund und Ländern sollten eingebracht und für die eigene Lebenswelt übersetzt werden. Kommunale Cyberräume bieten eine Chance, Mehrwerte zu schaffen, müssen dabei aber auch die kommunale Identität wahren.

Bernd Mutter  
Amtsleiter Bürgerservice und Informationsverarbeitung  
Stadt Freiburg

## Kommunaler Cyberraum

KLEINE UND MITTLERE KOMMUNEN KÖNNEN DIE  
DYNAMISCH WACHSENDEN SICHERHEITSANFORDERUNGEN  
KAUM EIGENSTÄNDIG BEWÄLTIGEN



### Zukunftslabor für "digitale Souveränität"

Ein kommunaler Cyberraum der lokalen Bürgergesellschaft wird dann gelingen, wenn die Kommunen die "digitale Souveränität" der Menschen achten und die Entwicklung der "digitaler Souveränität" mit anderen unterstützen und stärken. Das heißt: Im Sinne von Hermann Hill ("Aus Daten Sinn machen") geht es auch darum, die Analyse- und Deutungskompetenzen der Bürger in der Welt von Big Data und Open Data zu stärken, um neue Bildung, neue Modelle der Partizipation und Zusammenarbeit als stetigen sozialen Lernprozess zu ermöglichen.

Der kommunale Cyberraum ist hier eine Hilfe, um Antworten auf entscheidende Fragen zu entwickeln: Wie kann sich der Mensch in den neuen riesigen Datenwelten zurechtfinden? Wie können wir in diesen Datenwelten sicher, gut und hilfreich zusammenleben? Und welchen Beitrag zur Orientierung können Kommunen als "digitale Dienstleister" an der Schnittstelle zwischen Staat und Zivilgesellschaft hierbei leisten? Das sind neue Soziale Fragen für vorausschauende Städte und Gemeinden als Zukunftslabore.

Hans-Josef Vogel  
Bürgermeister der Stadt Arnsberg

## NEUE VERTRAUENS-RÄUME SIND ERFORDERLICH

Mit der Entwicklung von digitalen Dienstleistungszentren kommt es mehr denn je darauf an, im Internet Vertrauensräume aufzubauen, mit denen Vertraulichkeit, Verfügbarkeit und Integrität der Kommunikation zwischen Verwaltung, Politik und Zivilgesellschaft gesichert sind.

- Die Entwicklung vertrauenswürdiger Infrastrukturen und Dienste im nationalen und europäischen Kontext wird nur gelingen, wenn die besondere Rolle und die Anforderungen der Kommunen dabei berücksichtigt werden.
- Bei den komplexen Herausforderungen zur Entwicklung kommunaler Cyberräume sind Städte, Kreise und Gemeinden jedoch auch auf die Unterstützung von staatlichen Behörden angewiesen.
- Für die organisatorische, rechtliche und technische Gestaltung von Vertrauensinfrastrukturen ist deshalb das Zusammenwirken der relevanten Akteure aus Bund, Ländern und Kommunen erforderlich.

Die individuelle Aufgabenerledigung in Kommunen ist in ihren Verwaltungsprozessen kaum vergleichbar mit der Charakteristik von Steuerungsprozessen in staatlichen Behörden bei Bund und Ländern. Kommunale Organisationsexperten mahnen immer wieder an, dass IuK-Dienste, die sich auf der staatlichen Ebene bewährten – z. B. im elektronischen Dokumentenmanagement – für die differenzierten und kommunikationsintensiven Verwaltungsprozesse in kommunalen Dezernaten, Ämtern und Referaten nicht ohne Anpassungen geeignet sind.

Nur im Zusammenwirken aller Ebenen ist es möglich, die kommunalen Infrastrukturen zu sanieren und somit für den sicheren Umgang mit Daten von Bürgerschaft und Wirtschaft fit zu machen. Der hohe Bedarf an Abstimmung und Zusammenarbeit zu technischen, organisatorischen und rechtlichen

Aspekten wird deutlich mit Blick auf die aktuelle Situation im kommunalen E-Government:

- Von den ca. 300.000 IT-Servern, die in kommunalen Verwaltungen stationär in Betrieb sind, befinden sich nur etwa die Hälfte – so der frühere CIO der Hessischen Landesregierung, Horst Westerfeld – in speziell gesicherten Räumlichkeiten.
- Der vom Bundesamt für Sicherheit (BSI) empfohlene Grundschutz, der für den Betrieb sicherer IuK-Infrastrukturen unabdingbar ist, kann allein vor dem Hintergrund ihrer Verwaltungskraft nicht von allen Kommunen eigenständig realisiert werden.
- Mit der Nutzung der vorhandenen Instrumente zur Gestaltung sicherer Infrastrukturen (De-Mail, nPA, Governikus, etc.) fühlen sich IT- und Sicherheitsverantwortliche aus vielen Städten und Gemeinden bereits heute belastet.
- Für die interkommunale und ebenenübergreifende Zusammenarbeit zur Realisierung effizient und integriert aufgebauter sicherer Infrastrukturen sind Städte, Kreise und Gemeinden aufgrund fehlender Handlungsempfehlungen und Standards nicht ausreichend vorbereitet. In einer Vielzahl von Regionen ist die interkommunale Zusammenarbeit auf länderübergreifende Abstimmungen und Standards angewiesen, die ebenfalls noch zu schaffen sind (z.B. Berlin/Brandenburg, Hamburg/Niedersachsen/Schleswig-Holstein, Metropolregion Rhein-Neckar).
- Auch für eine effiziente und sichere Nutzung des deutschlandweiten DOI-Netzes, das bereits ab Januar 2015 zur Verfügung steht, fehlen in vielen Kommunen wesentliche Voraussetzungen.

### Ressourcen schonen

In Zeiten des demografischen Wandels und der Konsolidierung kommunaler Haushalte können kleine und mittlere Städte und Gemeinden die dynamisch wachsenden Anforderungen an IuK-Sicherheitsinfrastrukturen kaum eigenständig bewältigen. Für die 11.000 kreisangehörige Städte und Gemeinden ist es künftig nicht mehr darstellbar, die entsprechenden Experten zu gewinnen.

Statt improvisierter Lösungen sollten mit der Entwicklung standardisierter kommunaler Cyberräume neue professionelle Wege gefunden werden, um durch interkommunale Kooperationen bzw. Ebenen-übergreifende IuK-Infrastrukturen die Personal- und Finanzressourcen der Kommunen zu schonen.

Das bedeutet: der Mehraufwand für den professionellen Betrieb kommunaler Cyberräume muss kompensiert werden durch Effizienzgewinne von Ebenen-übergreifenden bzw. interkommunalen Infrastrukturen.

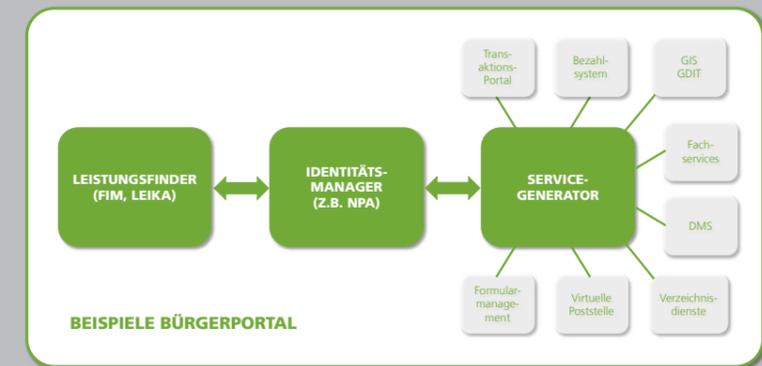
Städte, Kreise und Gemeinden müssen in der Lage sein, sich stärker um ihr Kerngeschäft kümmern zu können und weniger um sicherheitstechnische Probleme.

Jörg-Michael Schrader  
Kämmerer der Stadt Freudenberg

# KOMMUNALER CYBERRAUM SCHAFFT EFFIZIENZGEWINN

Technologische und organisatorische Voraussetzung sind Kommunale Cyberräume als Kommunikationsplattform. Die nötigen Technologien sind zu großen Teilen bereits vorhanden, sie müssen intelligent integriert und Ergänzungen noch entwickelt werden.

Abbildung 1: Für die effiziente Entwicklung von Kommunalen Cyberräumen ist zu klären, welche Dienste vom Bund bzw. von den jeweils zuständigen Ländern den Kommunen für ihre Aufgabenerledigung unter technischen, organisatorischen bzw. rechtlichen Aspekten zur Verfügung gestellt werden können



## Regeln, Prozesse und Standards

Kommunale Cyberräume erfordern neben technischen Komponenten gleichermaßen Daten und Wissen der Verwaltung sowie Regeln, Prozesse und Standards für ihren Einsatz. Passgenaue E-Services erfordern das Zusammenwirken aller Kommune 2.0-Akteure. Der kommunalen Seite obliegt das Erarbeiten neutraler fachlicher Anforderungen an E-Services - deren Realisierung und Angebot übernehmen die innovativen Kräfte des Marktes. Bund und Land unterstützen zweckmäßig durch die Bereitstellung technischer E-Services (Payment, Netz, Formulare,...), aber auch mit standardisiertem und harmonisiertem Verwaltungswissen („Straßen“, „Adressen“, „Liegenschaften“ etc).

Sachsen ist für die Ebenen-übergreifende Kooperation gut gerüstet: die SAKD als Kompetenzzentrum für kommunale „E-Service-Infrastrukturen“, der Sächsische IT-Kooperationsrat für die institutionalisierte Zusammenarbeit zwischen Land und Kommunen sowie die anstehende politische Wegweisung mit einem E-Government-Gesetz bilden den rechtlichen, organisatorischen und technischen Rahmen für kommunale Cyberräume und anspruchsvolle E-Service-Architekturen.

Thomas Weber  
Direktor  
Sächsischen Anstalt für kommunale Datenverarbeitung

## VON DER SILOINNOVATION ZUM BÜRGERPORTAL

Für die Informationssicherheit werden vom Bundesministerium des Innern, vom Bundesamt für Sicherheit in der Informationstechnologie sowie von kommunalen IT-Dienstleistern bereits eine Vielzahl an Sicherheitskomponenten und Standards angeboten bzw. verbindlich vorgeschrieben, die unterschiedliche technische bzw. organisatorische Funktionen erfüllen:

- BSI-Grundschutz
- DOI-Netz
- IPv6
- Governikus, OSC etc
- Neuer Personalausweis (nPA)
- De-Mail
- Prozessdatenbeschleuniger P23R
- Föderales Informationsmanagement (FIM) / D115

Diese Vielfalt an technischen und organisatorischen Komponenten ist für die mehr als 11.000 Kommunen in ihren Auswirkungen auf die bestehenden Infrastrukturen im Einzelnen nicht immer erkennbar bzw. beherrschbar.

Das Fraunhofer Institut FOKUS und Kommune 2.0 e. V. bieten eine Plattform für die Entwicklung von Migrationsempfehlungen zu offenen Sicherheitsarchitekturen und -infrastrukturen. Es ist an der Zeit, Eckpunkte für eine integrierende Referenzarchitektur zu entwickeln – ausgehend von aktuellen Sicherheitsrichtlinien (BSI-Grundschutz) und verfügbaren Sicherheitsinfrastrukturen (DOI, OSCI, ...) sowie zukunftsweisenden Konzepten wie DOI 2015, OSCI 2.0, Software as a Service (SaaS), Cloud-Technologien etc..

Die Eckpunkte einer offenen Referenzarchitektur sollen zur 2. Kommune 2.0-Sicherheitskonferenz bis Oktober 2014 mit dem Ziel entwickelt werden, die unterschiedlichen Innovationsprojekte auf Bundes- und Länderebene im Sinne eines

integrierten Kommunalen Cyberraums zu synchronisieren, um somit die Umsetzung von Sicherheitsstandards zu vereinfachen und zu beschleunigen.

Für die Entwicklung der offenen Referenzarchitektur ist zuvorderst zu klären, welche technischen und organisatorischen Rahmenbedingungen die 16 Länder ihren Kommunen bereits bieten, um Städte, Kreise und Gemeinden in ihrer autonomen Aufgabenerledigung zu unterstützen und zugleich ebenen- und länderübergreifende Zusammenarbeit ermöglichen. Hierfür müssen individuelle Nutzungsszenarien für die Anbindung an das DOI-Netz Ebenen-übergreifend konzipiert und diskutiert werden, in Verbindung und Abstimmung mit länderspezifischen Sicherheitsinfrastrukturen bzw. -diensten, die u.a. von kommunalen IT-Dienstleistern angeboten werden.

Zu den erforderlichen Komponenten des Kommunalen Cyberraums und damit zu den Bestandteilen der Referenzarchitektur gehören u. a.:

- Standards für die Leistungsfindung (FIM, Leika, Service D115)
- Anwendungsbezogene Nutzung von nPA, De-Mail, Governikus, XÖV-Lösungen, etc. als sichere Kommunikationsinfrastrukturen sowie für das Identitätsmanagement
- Standards für allgemeine Verwaltungsdienste (u.a. intelligente Formularserver, DMS, Online-Bezahlfunktionen)
- Standards und Infrastrukturen für den Ausbau von Kommunikationsdiensten unter Nutzung raumorientierter Informationsservices (INSPIRE, GDI-DE)
- Sicherheitsstandards für mobile eGovernment-Anwendungen
- Optionen zur Integration von P23R-Lösungen für den automatisierten sicheren Austausch von Informationen zwischen Wirtschaft und Verwaltung
- Sicheres Routing von vertraulichen Informationen durch IPv6-Standards
- Szenarien zur Nutzung des DOI-Netzes
- Standards für die Langzeitarchivierung



# VERNETZUNG IN KOOPERATIVEN ENTWICKLUNGSVERBÜNDEN

Kommunale Cyberräume sind erfolgskritisch für die Nationale E-Government-Strategie. Organisatorische Voraussetzung ist deshalb die schrittweise Vernetzung in kooperativen Entwicklungsverbänden über die staatlichen und die kommunalen Ebenen hinweg.

## EBENEN-ÜBERGREIFENDE KOOPERATION FÜR DEN KOMMUNALEN CYBERRAUM

Der Erfolg nationaler E-Government-Strategien ist insbesondere abhängig von sicheren interoperablen IuK-Infrastrukturen im kommunalen Raum. Daher liegt die Entwicklung von kommunalen Cyberräumen auch im Interesse des Bundes und der Länder, um

- den technisch-organisatorischen „Vertrauensraum“ für Bürgerschaft und Wirtschaft zu schaffen,
- der Rolle der Kommune als Knotenpunkt für digitale Information und Kommunikation gerecht zu werden – auch im Wettbewerb mit privatwirtschaftlich organisierten Informations- und Kommunikationsdiensten,
- nachhaltig die Leistungsfähigkeit der kommunalen Verwaltung in Zeiten des demografischen Wandels – und den damit verbundenen personellen Engpässen – sicher zu stellen,
- die Aktivierung und Beteiligung von Bürgerschaft und Wirtschaft bei der Lösung aktueller politischer Herausforderungen (u. a. Bildungsinitiativen, Energiewende, Leben im Alter, soziale Integration) zu ermöglichen,
- die IuK-Sicherheitsinfrastrukturen aus vorhandenen Einzelprojekten bzw. „Insellösungen“ im Sinne integrierter kommunaler Cyberräume zu definieren und zu entwickeln,
- die Wettbewerbsfähigkeit regionaler Wirtschaftsräume zu erhöhen.

Zu klären ist, inwieweit das Konnexitätsprinzip Länder noch davon abhält, kommunale IuK-Infrastrukturen im Sinne kommunaler Cyberräume materiell zu unterstützen bzw. landesweite Sicherheitsinfrastrukturen bereitzustellen. In die damit verbundenen Berechnungen sind neben den unzweifelhaft entstehenden Errichtungskosten insbesondere auch die mittel- und langfristigen Nutzeneffekte für Kommunen bei Anwendung neuer Lösungen zu berücksichtigen.

Bisher sind die technischen Infrastrukturen – den traditionellen föderalen Autonomieregelungen entsprechend – zumeist heterogen auf Bundes-, Länder- und Kommunalebene verteilt und oft auch als „Insellösungen“ organisiert. Es gilt zeitnah einen Diskurs anzustoßen, der die Sicherheitsaspekte von IuK-Infrastrukturen im Ebenen-übergreifenden Dialog neu bewertet und ordnet, um zu kosteneffizienten Lösungen zu kommen, die zugleich die kommunale Autonomie berücksichtigen.

### Eckpfeiler für das Vertrauen in die Sicherheit

Die Herausforderungen in der Informationssicherheit können Bund, Länder und Kommunen nur gemeinsam lösen. Die Kommunen müssen als wichtige Knotenpunkte zwischen Zivilgesellschaft, Wirtschaft und öffentlicher Verwaltung genauso in die Pflicht genommen werden, wie Länder und Bund. Modelle für den kommunalen Cyberraum müssen die Gewährleistung der Informationssicherheit Ebenen-übergreifend ermöglichen. Dies geht nur auf Basis gemeinsamer sicherer Infrastrukturen wie dem Verbindungsnetz, professioneller eigener IT-Dienstleister und einem einheitlichen Informationssicherheitsmanagement nach BSI-Standards. Eine weitergehende Professionalisierung, Konsolidierung und Zusammenarbeit in der IT wird daher unumgänglich sein. Gleichzeitig wird die Zertifizierung und Zulassung durch bzw. nach Anforderungen des BSI ein wichtiger Eckpfeiler für das Vertrauen in die tatsächliche Sicherheit von IT-Produkten sein müssen.

Dr. Stefan Grosse  
Referatsleiter IT 5  
IT-Infrastrukturen, IT-Sicherheitsmanagement des Bundes  
Bundesministerium des Innern,

## DIE ROLLE DES BUNDES

Um die Entwicklung kommunaler Cyberräume zu beschleunigen, ist die Entwicklung von Migrationsempfehlungen und einer Ebenen-übergreifenden Referenzarchitektur zur Gestaltung integrierter kommunaler Cyberräume erforderlich, die den Kommunen hilft, Infrastrukturen aufzubauen bzw. zu nutzen, die grundlegenden Sicherheitsanforderungen genügen. Sie sollen unter Einbeziehung der relevanten Stakeholder aller Ebenen definiert werden und sich dabei auf die bundesweit bereits verfügbaren Sicherheitsinfrastrukturen stützen (u. a. BSI-Grundschutz, DOI-Netz, OSCI / Governikus, De-Mail).

- 1 Um die erforderliche Interoperabilität von sicheren Cyberräumen in den verschiedenen Regionen, Ländern, beim Bund und im Kontext der EU sicher zu stellen, ist eine integrierende Standardisierung erforderlich, die auf den bisherigen internationalen IuK-Standards, dem XÖV-Framework, OSCI sowie übergreifenden Architekturkonzepten und Empfehlungen aus SAGA aufsetzen muss. Es gilt, diejenigen Standards zu identifizieren bzw. einzuordnen, die für die Gestaltung sicherer kommunaler Cyberräume relevant sind. Damit soll zugleich die für kommunale Anwender und Nutzer unübersichtliche Situation überwunden werden.
- 2 Der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) geforderte BSI-Grundschutz, und, soweit erforderlich, die Zertifizierung nach ISO 27001, die für den Betrieb sicherer IuK-Infrastrukturen unabdingbar sind, sollen speziell für den kommunalen Cyberraum definiert und verständlich eingeordnet werden.
- 3 Die Migrationsempfehlungen sowie die Sicherheitsarchitekturen und -Infrastrukturen gewährleistet zuallererst, dass Städte, Kreise und Gemeinden in ihrer autonomen Aufgabenerledigung durch einfach einsetzbare sichere IuK-Infrastrukturen im kommunalen Cyberraum unterstützt werden.
- 4 Darüber hinaus sollen mit den Ländern die Effizienzpotenziale erschlossen werden, die mit einer Ebenen-übergreifenden bzw. interkommunalen Zusammenarbeit zu erzielen sind.

- 5 Mit dieser Zielsetzung gilt es, IuK-Sicherheitsinfrastrukturen aus vorhandenen Einzelprojekten bzw. „Insellösungen“ im Sinne integrierter kommunaler Cyberräume zu definieren, zu entwickeln und anwendungsbezogen zur Verfügung zu stellen.



### Der Dialog hat schon begonnen

In Rheinland-Pfalz hat der Dialog zur Entwicklung kommunaler Cyberräume bereits begonnen. Grundlage hierfür ist eine Entwicklung des Landesbetriebs Daten und Information Rheinland-Pfalz (LDI), dem zentralen IT-Dienstleister des Landes. Als technische neue Plattform wurde durch den LDI eine Private Cloud für Fachverfahren verschiedener Organisationen auf Landesebene aufgebaut. Der LDI hat damit unter dem derzeitigen Service-Modell „Platform as a Service (PaaS)“ eine moderne, sichere und kosteneffiziente Lösung für die öffentliche Verwaltung des Landes Rheinland-Pfalz geschaffen.

Der LDI gibt damit die technologische Antwort die steigende Nachfrage der öffentlichen Verwaltung nach zentralisierten Dienstleistungen mithilfe von Cloud Computing ressourcenschonend zu bedienen. Mit diesem technologischen Ansatz kann die Forderung der sicheren Gestaltung eines kommunalen Cyberraumes entwickelt werden, die mit einer Professionalisierung und Konsolidierung kommunaler Infrastrukturen einhergehen kann. Die Private Cloud des LDI kann die Rolle einer vertrauenswürdigen Kommunikationsplattform zur Schaffung kommunaler Cyberräume darstellen.

Staatssekretärin Heike Raab  
Ministerium des Innern, für Sport und Infrastruktur  
Rheinland-Pfalz

**VORAUSSETZUNG FÜR FÖDERALE KOOPERATIONEN  
IST DIE VEREINFACHUNG VON  
STANDARDS FÜR KOMMUNALE CYBERRÄUME**

Abbildung 2: Um die erforderliche Interoperabilität von sicheren Cyberräumen in Städten, Kreisen und Gemeinden, in Ländern sowie beim Bund im Kontext der EU-Richtlinien sicher zu stellen, ist eine integrierende Standardisierungsstrategie erforderlich.



## DIE ROLLE DER LÄNDER

Die Ausgangssituation der Länder in organisatorischer, rechtlicher wie auch technischer Hinsicht ist derzeit noch sehr unterschiedlich. Mehrere Landesregierungen (u. a. Bayern, Niedersachsen und Sachsen) unterstützen Kommunen bereits beim Aufbau sicherer Infrastrukturen. Diese Lösungen lassen derzeit jedoch noch keine länderübergreifenden Sicherheitsstrategien zu.

Mit der offenen Referenzarchitektur für Kommunale Cyberräume soll – eingehend auf die unterschiedlichen Rahmenbedingungen der Länder – die Grundlage für Migrationsstrategien entwickelt werden, die den nationalen bzw. europäischen Vorgaben entsprechen.

Sie ermöglicht Kommunen bzw. kommunalen IT-Dienstleistern frühzeitig eine zukunftssichere Planung beim Aufbau integrierter IuK-Infrastrukturen und -dienste zum Betrieb kommunaler Cyberräume.

Beispiel Bayern: Bayern betreibt ein eigenes Behördennetz das neben staatlichen Einrichtungen auch den Kommunen offen steht. Für die erforderliche Vertraulichkeit bei der Datenübermittlung innerhalb des Bayerischen Behördennetzes sorgen eine Leitungsverchlüsselung sowie eine PKI, die Authentifizierungs-, Verschlüsselungs-, Signatur- und Maschinenzertifikate bereitstellt. Die angeschlossenen staatlichen und kommunalen Stellen sind in ein Informationssicherheitsmanagement mit festgelegten Zuständigkeiten, Prozessen und Meldewegen eingebunden. Alle Behördennetzteilnehmer werden bei Sicherheitsvorfällen durch ein Landes-CERT (Computer Emergency Response Team) unterstützt. Eine zentrale Sicherheitsinstanz am Übergang des Behördennetzes zum Internet schützt die Teilnehmer vor Angriffsversuchen aus dem Internet.



### Bis zu 36.000 Angriffseignisse – täglich!

Mit der Umsetzung von elektronischen Dienstleistungen bergen die Netze unserer Informationsgesellschaft auch Daten von unschätzbarem Wert. Es ist daher nicht verwunderlich, dass die organisierte Kriminalität diesen Werten auflauert. Alleine die Sensoren am Bayerischen Behördennetz melden täglich bis zu 36.000 Ereignisse, die auf Angriffsversuche hindeuten. Diese beeindruckende Zahl macht klar: IT-Sicherheit ist eine Kernaufgabe in der Informationsgesellschaft.

Kommunale Cyberräume werden deshalb von lokalen Bürgergesellschaften auch nur dann angenommen, wenn sich die Kommunen professionell um die Sicherheit ihrer Cyberräume bemühen und Bund und Länder die Kommunen in ihre Sicherheitsprozesse einbinden. Der IT-Planungsrat hat hierfür den Grundstein mit der für Bund und Länder verbindlichen Leitlinie für Informationssicherheit gelegt. Darauf aufbauend eröffnen sich nun Möglichkeiten zur Professionalisierung und Konsolidierung von IT-Infrastrukturen, die es den Kommunen ermöglichen, länderspezifisch von Ebenen-übergreifenden Sicherheitsinfrastrukturen zu profitieren.

Dr. Andreas Mück  
IT-Sicherheitsbeauftragter für den Freistaat Bayern  
Bayerisches Staatsministerium der Finanzen

## DIE ROLLE VON KREISEN UND KREISFREIEN STÄDTEN

Städte und Kreise gestalten gemeinsam mit kommunalen IT-Dienstleistern integrierte Infrastrukturen für Kommunale Cyberräume – entsprechend regionaler Anforderungen und Gegebenheiten auf Basis nationaler Sicherheitsstandards und der von den Ländern zur Verfügung gestellten bzw. vorgegebenen Sicherheitsinfrastrukturen und -dienste.

## DIE ROLLE VON KREISANGEHÖRIGEN STÄDTEN UND GEMEINDEN

Kreisangehörige Städte und Gemeinden konzentrieren sich auf ihre Kernkompetenzen und nutzen ihre Fachanwendungen und -dienste im technologischen Umfeld der von den Ländern bzw. von Kreisen angebotenen kommunalen Cyberräume.

## DIE ROLLE VON ÖFFENTLICHEN UND KOMMUNALEN IT-DIENSTLEISTERN

Die oben angeführte Komplexität der Ebenen-übergreifenden Kommunikation, der vertikalen Vernetzung zwischen den Verwaltungen und die notwendige Implementierung von Shared-Services bzw. die Trennung in Front- und Backoffices erfordert eine gemeinsame Anstrengung, um die Rolle von IT-Dienstleistern im Sinne von Service Providern zu schärfen. Im Mittelpunkt des Rechenzentrums 2.0 stehen Dienstleistung, Beratung und Organisationsunterstützung inklusive definierter Leistungsmessung, Personalstellung und Einbeziehung von politischen Verantwortungsträgern in die Aufgabendefinition.



### Mindestsicherheits-Niveau für alle Ebenen

Es ist unbestritten, dass auch im kommunalen Bereich IT-Sicherheit zu gewährleisten ist und überwiegend auch gewährleistet wird. Neben den unmittelbaren Maßnahmen der IT-Sicherheit ist aber auch das Thema „Vertrauenskultur“ zwischen dem Land und den Kommunen nicht außer Acht zu lassen und zu stärken.

Ein zwischen dem Land und dem kommunalen Bereich gemeinschaftlich zu definierendes und zu vereinbarendes Mindest-Sicherheitsniveau bietet die Grundlage für die vertrauensvolle Zusammenarbeit. Fortlaufende Sensibilisierungsmaßnahmen, die sich an alle Hierarchieebenen richten, ergänzen dieses Mindest-Sicherheitsniveau und sorgen für die nötige Akzeptanz.

Die Einbindung der niedersächsischen Kommunen in das vom Land Niedersachsen betriebene N-CERT und der gegenseitige Informationsaustausch hierbei ist eine grundlegende Säule für die gemeinschaftliche Abwehr von Gefahren aus dem Cyberraum. Die Frage, bis zu welcher kommunalen Ebene eine unmittelbare Einbindung sinnvoll und geboten ist, bedarf noch der Klärung.

Manfred Malzahn  
Niedersächsischer Landkreistag

# PERSPEKTIVE BRÜSSEL

Die kommunale Ebene steht in direkter Wechselwirkung mit den Zielen und Maßnahmen der Europäischen Union.



## KOMMUNALE CYBERRÄUME BIETEN DIE GRUNDLAGE ZUR UMSETZUNG DES EUROPÄISCHEN E-GOVERNMENT-AKTIONSPLANS 2011–2015

### Ziele des Europäischen E-Government-Aktionsplans 2011–2015

- Stärkung der Bürgerschaft und Unternehmen durch elektronische Behördendienste, die ganz auf die Bedürfnisse der Nutzer abgestimmt sind und in Zusammenarbeit mit Dritten entwickelt wurden, sowie durch einen verstärkten Zugang zu öffentlichen Informationen, gesteigerte Transparenz und wirksame Mittel zur aktiven Beteiligung an politischen Entscheidungsprozessen,
- Erleichterung der Mobilität im Binnenmarkt durch nahtlose elektronische Behördendienste, um Unternehmensgründungen, das Studieren, Arbeiten, Wohnen und das Leben für Rentner in der Europäischen Union zu vereinfachen,
- Effizienz und Effektivität durch das stetige Bemühen, mit Hilfe elektronischer Behördendienste die Verwaltungslasten zu verringern, organisatorische Abläufe zu verbessern und eine nachhaltige, kohlenstoffarme Wirtschaft zu fördern,

Quelle: KOM(2010) 743

Das Vorhaben Kommunaler Cyberraum unterstützt den Informationsaustausch zwischen der kommunalen Ebene über die Ebenen bis zur EU sowohl in Bezug auf die Vermittlung der strategischen Ziele und Regulierungen der EU als auch in Bezug auf die Vertretung der kommunalen Interessen über die Ebenen hinweg.

DER EUROPÄISCHE-GOVERNMENT-AKTIONSPLAN WIRD DEN BEHÖRDEN HELFEN, DURCH EINSATZ VON IUK-TECHNOLOGIEN BESSERE DIENSTLEISTUNGEN ZU NIEDRIGEREN KOSTEN ZU ERBRINGEN, UM DEN BÜRGERINNEN, BÜRGERN UND UNTERNEHMEN MIT EINEM BESSEREN ZUGANG ZU ÖFFENTLICHEN DIENSTEN DAS LEBEN ZU ERLEICHTERN.

NEELIE KROES, KOMMISSARIN FÜR DIE DIGITALE AGENDA  
ZUSTÄNDIGE VIZEPRÄSIDENTIN DER EU-KOMMISSION

### Relevante EU-Regulierungen

Bei der EU-Regulierung wird zwischen zwei Instrumenten der Gesetzgebung unterschieden: der Richtlinie (RL), die von den Mitgliedstaaten in eigenen Gesetzen umzusetzen sind, und Verordnungen (VO), die wie deutsches Bundesrecht direkt anzuwenden sind und zu denen keine nationalen Sonderregelungen erlassen werden dürfen.

#### Dienstleistungs-RL

Ziel ist eine freie grenzüberschreitende Erbringung von Dienstleistungen innerhalb der EU zu ermöglichen und bürokratische Hemmnisse abzubauen. Ein Mittel hierfür ist der Einheitliche Ansprechpartner, der eine elektronische Verfahrensabwicklung ermöglicht. Die Umsetzung des letzten Punktes ist weitgehend erfolgt. Die Nutzung dieses Einheitliche Ansprechpartners ist noch recht verhalten.

#### elektronischeVergabe-RL

Die neue RL 2014/24, welche die Vergabe RL von 2004 ablöst, ist im Februar 2014 in Kraft getreten und muss bis April 2016 in deutsches Recht umgesetzt werden. Mit dieser RL – als einer von dreien – soll das Vergaberecht modernisiert werden, indem der Ausbau der elektronischen Auftragsvergabe als Standardvergabeverfahren in Europa vorangetrieben wird.

#### elektronischeRechnungs-RL

Die Möglichkeit von elektronischen Abrechnungen ist seit Jahren europaweit wie auch national geregelt. Aufgrund des technischen Fortschritts sind immer wieder Anpassungen notwendig. Die jüngste erfolgte per RL Anfang 2014. Die dort beschriebenen Formate entsprechen beispielsweise auch dem in Deutschland entwickelten ZUGFeRD, als einfachstem Datenformat für den Versand von elektronischen Rechnungen.

#### eIDAS-VO

Die VO über elektronische Identitäten, Authentisierung und Signaturen sollte ursprünglich nur die Signaturrechtlinie von 1999 ablösen. Die VO wird 2016 in Kraft treten. Neben elektronischen Signaturen, Zeitstempeln und Organisationszertifikaten, wird auch die eID, wie sie in Deutschland auf dem neuen Personalausweis, dem elektronischen Aufenthaltstitel oder der elektronischen Gesundheitskarte vorhanden ist, europaweit geregelt. Auch für registrierte elektronische Zustelldienste, wie der De-Mail, wird es neue, europaweite Regelungen geben. Das deutsche Signaturgesetz wird durch die VO abgelöst. Die Auswirkungen auf das De-Mail- und andere Gesetze ist zu beachten.

#### Datenschutz-GVO

Die geplante DS-GVO soll die alte EU Datenschutz-RL von 1995 ersetzen. Alle nationalen Datenschutzgesetze, wie das deutsche BDSG, würden dann aufgehoben. Mit der DS-GVO soll die Verarbeitung von personenbezogenen Daten durch private Unternehmen EU-weit vereinheitlicht werden. Bekannte Ideen aus der DS-GVO sind das Recht auf Vergessenwerden und das Recht auf Datenportabilität.

# INITIATIVE „KOMMUNALER CYBERRAUM“ HANDLUNGSBEDARF

FÜNF HANDLUNGSFELDER FÜR DEN AUFBAU VON  
DIGITALEN VERTAUENSÄUMEN FÜR BÜRGERSCHAFT,  
WIRTSCHAFT, POLITIK UND VERWALTUNG

## 1. RAHMENBEDINGUNGEN

Evaluierung von Anforderungen, Nutzenpotentialen und Rahmenbedingungen für Kommunale Cyberräume

- Definition Kommunaler Cyberraum als „digitaler Vertrauensraum“
- Darstellung heutiger Risiken und Nutzenpotentiale für Bürgergesellschaft, Unternehmen, Verwaltung und Politik
- Erstellung einer Bestandsaufnahme zu politischen, rechtlichen, organisatorischen und technischen Rahmenbedingungen für die Ebenen-übergreifende Umsetzung in Bezug auf 16 Länder
- Evaluierung von Anforderungen aus Sicht der relevanten Stakeholder an erforderliche IuK-Infrastrukturen und Dienste für Bürgergesellschaft, Unternehmen, Verwaltungen und Politik

**Ergebnisziele:**

- Definition des Vorhabens „Kommunaler Cyberraum“ mit Darstellung von Risiken und Nutzenpotentialen
- Darstellung der Anforderungen an IuK-Infrastrukturen und Dienste für „digitale kommunale Vertrauensräume“
- Darstellung der Rahmenbedingungen in 16 Ländern für die Ebenen-übergreifende Umsetzung Kommunaler Cyberräume
- Empfehlungen für Organisationsstrukturen zur Umsetzung interkommunaler und Ebenen-übergreifender Zusammenarbeit.

## 2. REFERENZARCHITEKTUR

Erarbeitung einer offenen Ebenen-übergreifenden Referenzarchitektur für gesicherte IuK-Infrastrukturen und Dienste des Kommunalen Cyberraums

- Identifikation von Sicherheitsanforderungen und Lösungsansätzen sowie Darstellung des Bezugs zu sicherheitstechnischen Anforderungen – u. a. BSI-Grundschutz, DOI-Netz, ITIL
- Identifikation der relevanten technischen Standards zur Umsetzung des Kommunalen Cyberraums
- Identifikation von technischen Rahmenbedingungen auf Bundesebene (z.B. Bereitstellung nationaler Infrastrukturen und Dienste wie DOI, D115, nPA, De-Mail), Länderebene (übergreifende Infrastrukturen und Dienste), kommunale Ebene (interkommunale Infrastrukturen und Dienste)
- Identifikation von Best Practice Beispielen für (Referenz-) Architekturen und IuK-Infrastrukturen und Dienste des Kommunalen Cyberraums
- Aktualisierung der Fraunhofer FOKUS eGov-Referenzarchitektur als eine Grundlage der Referenzarchitektur für Kommunale Cyberräume

**Ergebnisziele:**

- Aufbereitung der länderspezifischen technischen Rahmenbedingungen in Bezug auf IuK-Komponenten und Dienste aller Ebenen zur Umsetzung des des Kommunalen Cyberraums
- Eckpunkte einer Referenzarchitektur für sichere IuK-Infrastrukturen und Diensten des Kommunalen Cyberraums

## 3. MIGRATIONSTRATEGIEN

Entwicklung von länderspezifischen Migrationsstrategien zur Ebenen-übergreifenden Umsetzung Kommunaler Cyberräume unter Wahrung der kommunalen Autonomie

- In Bezug auf die jeweils autonomen (!) politischen, rechtlichen (eGovG, etc.) und organisatorischen Rahmenbedingungen der an dem Vorhaben beteiligten Länder
- In Bezug auf die E-Government-Infrastrukturen und -Dienste der an dem Vorhaben beteiligten Länder, die für den Aufbau Kommunaler Cyberräume genutzt werden können
- In Bezug auf die Identifikation und Darstellung von Musterlösungen für die an dem Vorhaben beteiligten Bundesländern, die die Umsetzbarkeit und den Nutzen Kommunaler Cyberräume für Bürgergesellschaft, Unternehmen, Verwaltungen und Politik aufzeigen
- In Kooperation mit kommunalen IT-Dienstleistern und den IT-Dienstleistern der Länder

**Ergebnisziele:**

- Länderspezifische Migrationsstrategien zur Entwicklung von Ebenen-übergreifenden IuK-Infrastrukturen und Diensten für die kosteneffiziente Nutzung von gesicherten Cyberräumen unter Wahrung der kommunalen Autonomie
- Darstellung von Musterlösungen aus den an dem Vorhaben beteiligten Ländern, die die Umsetzbarkeit und den Nutzen Kommunaler Cyberräume aufzeigen



# INITIATIVE „KOMMUNALER CYBERRAUM“ HANDLUNGSBEDARF

## 4. UMSETZUNGSSZENARIEN

Erarbeitung von Umsetzungsszenarien (Roadmaps für Pilotvorhaben) und Wirtschaftlichkeitsbetrachtungen für die kosteneffiziente Nutzung von gesicherten IuK-Infrastrukturen und Diensten der Kommunalen Cyberräume unter Wahrung der kommunalen Autonomie

- Identifikation von organisatorischen, technischen und rechtlichen Anforderungen an die betriebliche Nutzung von gesicherten IuK-Infrastrukturen und Diensten Ebenen-übergreifender Kommunalen Cyberräume unter Wahrung der kommunalen Autonomie
- Erarbeitung von landesspezifischen Umsetzungsszenarien
- Durchführung von Wirtschaftlichkeitsbetrachtungen im Kontext von zu identifizierenden Good Practice Projekten, die sich an dem Vorhaben Kommunalen Cyberraum beteiligen
- Darstellung des Bezugs zu Organisationsstrukturen von kommunaler IT-Dienstleistern und den IT-Dienstleistern der Länder
- Evaluierung von Cloud- und Software as a Service (SaaS) Modellen auf Länder- und Kommunalebene

### Ergebnisziele:

- Landesspezifische Umsetzungsszenarien (Roadmaps für Pilotvorhaben)
- Übergreifende Wirtschaftlichkeitsbetrachtungen auf Basis von zu identifizierenden Good Practice Projekten
- Betriebsszenarien und Organisationsstrukturen kommunaler IT-Dienstleister und IT-Dienstleistern der Länder für Ebenen-übergreifende Dienstleistungen
- Übersicht über Cloud- und SaaS-Modelle auf Länder- und Kommunalebene
- Übersicht über diesbezügliche rechtliche Rahmenbedingungen, die bei der Umsetzung der Pilotvorhaben zu beachten sind

## 5. KOMMUNIKATIONS- MASSNAHMEN

Aufbau einer übergreifenden Kommunikationsinitiative (Bund, Länder, Spitzenverbände, Landesverbände, Wirtschaft, Wissenschaft, Städte, Kreise und Gemeinden) zur Umsetzung Kommunalen Cyberräume für die digitale Daseinsvorsorge

- Entwicklung und Abstimmung einer Ebenen-übergreifenden Kommunikationsstrategie; abgeleitet von länderspezifischen Kommunikationsmaßnahmen
- Vorbereitung und Präsentation von Beiträgen für nationale Gremien wie IT-Planungsrat, Normenkontrollrat, Kommunale Spitzenverbände, Kommunalpolitische Vereinigungen etc.
- Entwicklung und Aufbau von länderspezifischen Beratungsangeboten, die den Nutzen Kommunalen Cyberräume für Bürgergesellschaft, Unternehmen, Verwaltungen und Politik aufzeigen – unterstützt vom Bund (Vorbild: regionale Breitbandberatung von Bund und Ländern)

### Ergebnisziele:

- Darstellung der Kommunikationsstrategie und erster Kommunikationsmaßnahmen
- Aufbau einer übergreifenden Kommunikationsinitiative
- Vorbereitung und Präsentation von Beiträgen für nationale und EU-Gremien
- Entwicklung und Aufbau von länderspezifischen Beratungsangeboten



Fraunhofer-Institut für  
Offene Kommunikationssysteme FOKUS  
Kompetenzzentrum ELAN  
Dr. Michael Tschichholz  
Kaiserin-Augusta-Allee 31  
10589 Berlin

Tel. +49 30 3463-7115  
Fax +49 30 3463-99 7115

elankontakt@fokus.fraunhofer.de  
www.fokus.fraunhofer.de

Kommune 2.0 e. V.  
Max Schulze-Vorberg  
Goslarer Ufer 35  
10589 Berlin

Tel. +49 171 120 35 37  
Fax +49 321 21 40 65 07

max.schulze-vorberg@kommune2-0.de  
www.kommune2-0.de