IT und Internet als kritische Infrastruktur

– vernetzte Sicherheit zum Schutz kritischer Infrastrukturen –

Herausgegeben von

Prof. Dr. Wolfgang König,

Prof. Dr. Radu Popescu-Zeletin

und

Prof. Dr. Utz Schliesky

Autoren:

Prof. Dr. Roman Beck

Dr. Jörg Caumanns

Jürgen Großmann

Dr. Ulrich Meissen

Prof. Dr.-Ing. Jochen Schiller

Dr. Sönke E. Schulz

Jens Tiemann

Jakob Tischer

Dr. Armin Wolf

Markus Wollina

Kiel 2014

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet unter http://dnb.ddb.de abrufbar.

ISBN: 978-3-936773-88-0

Verlag:
Lorenz-von-Stein-Institut für Verwaltungswissenschaften
an der Christian-Albrechts-Universität zu Kiel
Olshausenstraße 40
24098 Kiel

Verkaufspreis: 24,90 €

Vorwort

Themen, die das Internet betreffen, haben derzeit Hochkonjunktur. Die NSA-Affäre und damit verbunden die Ausspähung der Netze mittels PRISM, Tempora und anderen prägen die öffentliche Debatte. Die Netzpolitik fristet nicht länger ein Schattendasein, sie ist wie nie in den Medien präsent. Dieses neue Politikfeld betrifft vor allem Fragen, die mit Infrastruktur und Betrieb des Netzes, den über das Internet verbreiteten Inhalten und Angeboten zusammenhängen. Allen diesen Aspekten, auch den Diskussionen um Ausspähung und andere Bedrohungen der Privatsphäre, bspw. durch multinational agierende Konzerne, gemein ist jedoch eine Grundvoraussetzung, nämlich die Zuverlässigkeit und Verfügbarkeit „des Netzes“. Wirtschaft, Gesellschaft und vielfach auch staatliche Einrichtungen verlassen sich nur zu gern darauf, dass schon alles funktionieren wird, der Zugang zum und die Nutzung des Netzes so sicher sind wie der Strom aus der Steckdose.

Angesichts der zunehmenden Bedeutung des Internets für Individuen, Gesellschaft, Wirtschaft und Staat geht ein vom ISPRAT e. V. gefördertes Projekt in diesem Diskussionspapier folgenden Fragen nach: Inwiefern ist das Internet eine kritische Infrastruktur? Und welche Konsequenzen aus rechtlich-regulatorischer, technischer sowie organisationaler Perspektive sind mit einer entsprechenden Einordnung verbunden? Eine Zuordnung des Internets als essentielle Grundversorgung in einer technisierten Informationsgesellschaft erlaubt den Vergleich mit anderen für das Funktionieren einer Gesellschaft basalen Grundversorgungseinrichtungen. Hätte die NSA das Internet „abgeschaltet“, wäre die Welle der Empörung wohl ungleich größer gewesen. Zudem haben die Enthüllungen von *Edward Snowden* deutlich gemacht, dass wesentliche Teile der Kommunikationsinfrastruktur des Internets von privaten Unternehmen beherrscht werden und eben nicht die Integrität und Sicherheit bieten, von der viele Nutzer und Unternehmen bisher wie selbstverständlich ausgegangen sind.

Vor diesem Hintergrund haben sich Forscher von der Goethe-Universität Frankfurt, des Fraunhofer-Instituts für Offene Kommunikationssysteme FOKUS und des Lorenz-von-Stein-Instituts für Verwaltungswissenschaften an der Christian-Albrechts-Universität zu Kiel zusammengefunden, um ein erstes Diskussionspapier vorzulegen. Insbesondere der Teilaspekt der denkbaren Handlungsalternativen – rechtlicher, technischer und organisatorischer Art – kann keine abschließenden Antworten formulieren. Dies ist auch nicht beabsichtigt. Erforderlich ist ein intensiver fachübergreifender, intersektoraler wie interdisziplinärer Diskurs, zu dem ISPRAT in seiner Vernetzung von Wirtschaft, Wissenschaft und Verwaltung einen entscheidenden Impuls geben kann.

Die Dokumentation der Ergebnisse des Forschungsprojekts gibt Anlass, Dank zu sagen, und zwar vor allem an den ISPRAT e. V. und seinen Vorstandsvorsitzenden *Matthias Kammer* für die großzügige Förderung. Dank gilt aber auch für neue in-

terdisziplinäre Perspektiven. Zahlreiche Projekte der Vergangenheit, die eine Reaktion des Staates auf eine veränderte Wirklichkeit sind, haben gezeigt, dass die überkommenen Handlungsinstrumente, die oftmals eindimensional fokussiert waren, den neuen Herausforderungen nicht mehr gerecht wurden. Der beständige Austausch im ISPRAT-Forschungsverbund mit anderen Disziplinen zwingt in positiver Weise zu einer Auseinandersetzung mit anderen Facetten multipolarer Modernisierungsvorhaben und dazu, im Interesse einer nachhaltigen Modernisierung des Staates eine gemeinsame Sprache zu finden.

Gedankt sei zudem allen Mitarbeiterinnen und Mitarbeitern der Goethe-Universität Frankfurt, des Fraunhofer-Instituts für Offene Kommunikationssysteme und des Lorenz-von-Stein-Instituts, ohne deren tatkräftige Unterstützung das Forschungsprojekt nicht so erfolgreich verlaufen wäre. Die hervorragende interdisziplinäre Zusammenarbeit der beteiligten Forschungseinrichtungen hat das Entstehen dieser einzigartigen Analyse überhaupt erst ermöglicht.

Frankfurt/Berlin/Kiel, im März 2014

Prof. Dr. Wolfgang König

Professur für BWL, insbes. Wirtschaftsinformatik und Informationsmanagement

Geschäftsführender Direktor des House of Finance

Goethe-Universität Frankfurt

Prof. Dr. Radu Popescu-Zeletin

Inhaber des Lehrstuhls für Offene Kommunikationssysteme an der Technischen Universität Berlin

Leiter des Fraunhofer-Instituts für Offene Kommunikationssysteme FOKUS

Prof. Dr. Utz Schliesky

Vorstand des Lorenz-von-Stein-Instituts für Verwaltungswissenschaften an der Christian-Albrechts-Universität zu Kiel

Leiter des Forschungsbereichs Staatliches Innovationsmanagement

Direktor des Schleswig-Holsteinischen Landtags

Inhaltsübersicht

Abbildungsverzeichnis

A. Zusammenfassung der Ergebnisse

Vielfach wird über „kritische Infrastrukturen“ gesprochen, die es gerade in Zeiten von internationalem Terrorismus zu schützen gelte. Wurden bisher vor allem die Elektrizitätsversorgung, Wasserver- und Abwasserentsorgung sowie Verkehrs- und Telekommunikationsinfrastrukturen unter diesen Begriff gefasst, lenken Ausfälle von IT-Infrastrukturen und des Internets nun den Blick zunehmend auch auf diesen Bereich. Die zunehmende internetbasierte Vernetzung von Systemen, auf deren Funktionieren Staat, Gesellschaft, Wirtschaft und der Einzelne angewiesen sind, macht moderne, technisierte Informationsgesellschaften anfälliger. Nicht der physische Schutz von Einrichtungen, bspw. von Rechenzentren, Knotenpunkten und Backbone-Netzen, steht im Fokus, sondern die IT-Sicherheit, verstanden als die Fähigkeit, Angriffe von außen auf die IT-Systeme abzuwehren sowie die Fehleranfälligkeit aufgrund interner Unzulänglichkeiten zu minimieren.

Der erste Gedanke zur Realisierung dieses Anspruchs geht zumeist in Richtung technischer Schutzmaßnahmen – Firewalls, Antivirenprogramme, Zugangsbeschränkung und Rechtemanagement sind aber nur Grundvoraussetzungen des Funktionierens von IT-Systemen. Deswegen nimmt die nachfolgende Analyse einen breiteren Blick ein und widmet sich zugleich technischen, rechtlichen wie organisatorischen Fragen. Im Ergebnis ist nur ein Zusammenspiel von Recht, Organisation und Technik geeignet, die „Lebensadern“ der Informationsgesellschaft zu sichern. Kurz zusammengefasst lässt sich folgendes Bild von IT und Internet als kritischer Infrastruktur zeichnen:

- Der Begriff der kritischen Infrastruktur ist nicht abschließend definiert und kein Rechtsbegriff (dazu C.). Es sind aber Tendenzen zu einer zunehmenden rechtlichen Erfassung erkennbar. Im Interesse der Schutzbedürftigkeit der betroffenen Infrastruktureinrichtungen erscheint dies zielführend. Allerdings ist wie auch in der Vergangenheit auf die Entwicklungsoffenheit zu achten: Recht und Technik stehen in einem Wechselverhältnis, welches sich sowohl auf den Schutzgegenstand (welche technischen Einrichtungen sind kritische Infrastruktur?) als auch auf die technischen Schutzmaßnahmen auswirkt, die ggf. regulativ gefordert werden.
- Die Vielfältigkeit der technischen Infrastrukturen, auf denen das Internet basiert, und der Umstand, dass es nicht „das Internet“ als solches gibt (dazu D.), zwingen zu einer differenzierten Bewertung, ob und inwieweit das Internet bzw. die zugrundeliegenden Infrastrukturen und IT-Systeme ihrerseits „kritische Infrastrukturen“ sind (dazu E.):
  - IT als solche kann keine kritische Infrastruktur darstellen – sie ist allenfalls Mittel zum Zweck, niemals Selbstzweck. Insofern ist

immer nur diejenige IT „kritisch“ im hier relevanten Maßstab, die auch für eine andere kritische Infrastruktur zwingend erforderlich ist. Dies gilt bspw. für Steuerungseinrichtungen von Verkehrs-, Energie-, Entsorgungs- und Gesundheitsinfrastrukturen.

- Diese Grundannahme, dass IT nur im Kontext anderer kritischer Infrastrukturen diese besondere Bedeutung teilt, ist anerkannt und findet sich explizit auch im Entwurf des IT-Sicherheitsgesetzes. Allerdings erfasst dies nicht zugleich die Gesamtheit der IT-Infrastrukturen. Erforderlich ist eine „dreifache Relevanzprüfung“: in einem ersten Schritt ist ein bestimmter Infrastrukturbereich als „kritisch“ zu klassifizieren, wobei sich diese Einstufung – in Stufe zwei – lediglich auf die „systemrelevanten“ Teile dieser Infrastruktur bezieht. In einem dritten Schritt strahlt diese besondere Bedeutung auf die für den maßgeblichen Teil der Infrastruktur maßgeblichen IT-Systeme aus.
- Daneben lässt sich aber auch festhalten, dass zumindest Teile des Internets, vor allem der Telekommunikationsinfrastruktur, auf der es basiert, aufgrund der Bedeutung – nicht für andere kritische Infrastrukturen, sondern allgemein für das gesellschaftliche, wirtschaftliche Leben – als kritische Infrastruktur einzustufen sind. Wie bei anderen kritischen Infrastrukturen strahlt dies dann auch auf diejenigen IT-Strukturen aus, die für die Funktionsfähigkeit des Internets erforderlich sind.

- Versucht man, sich Szenarien des Ausfalls kritischer Infrastrukturen auszumalen, liegt zu Beginn folgende Frage nahe: Was passiert eigentlich konkret, wenn das Netz längerfristig, vielleicht flächendeckend nicht erreichbar bzw. in seiner Zuverlässigkeit massiv eingeschränkt ist? Verlässliche Angaben dazu, wie wahrscheinlich dies ist, existieren nicht. Ist die Dezentralität des Internets einerseits seine große Chance, sich auch gegenüber Ausfällen zu bewähren, da sich die Informationen dann – ggf. verlangsamt – den noch vorhandenen „Weg“ suchen, ist sie andererseits auch seine Schwäche, da sie belastbare Risikoaussagen erschwert. Bei einer Abdeckung von 67,3 % der privaten Breitbandanschlüsse durch die drei größten Internet-Provider in Deutschland ist davon auszugehen, dass deren Ausfall auch den Zugang von 18 Millionen Anschlüssen (und damit ca. 36 Millionen Menschen) zum Netz verschließen würde. Dieses Szenario auf einige Stunden und ggf. Tage ausgedehnt dürfte u. a. zu folgenden Entwicklungen führen: zunächst Ausfall der Kommunikationsmöglichkeiten, die auf der Funktionsfähigkeit des Internet aufbauen (also E-Mail, Skype, Internettelefonie), steigende Nervosität der Nutzer – auch vor dem Hintergrund, dass große Teile der Medien- und Regierungskommunikation in Rich-

tung Bürger, die in Zukunft immer mehr auf das Internet (Webseiten, Internet-TV und Internet-Radio) verlagert werden, nicht mehr funktionieren. Bevorstehender Zusammenbruch der Finanzwirtschaft, da Finanzmarkttransaktionen überwiegend digital vorgenommen werden, ebenso wie beim automatisierten Computerhandel. Per Internet gesteuerte öffentliche Infrastrukturen brächen zusammen, kein Flugzeug könnte mehr abheben, Bankautomaten würden kein Geld mehr ausgeben, Buchungsvorgänge am Schalter wären ebensowenig möglich. Die Lebensmittelversorgung wäre durch ausfallende Kassen und Lagerlogistiksysteme ebenso gefährdet wie durch den Zusammenbruch der in hohem Maße vom Internet abhängigen Logistik- und Transportkette insgesamt. Um den bereits binnen Stunden für jeden spürbaren Folgen zu begegnen, hülfe nur noch ein erfolgreiches Krisenmanagement – das indes ebenfalls zumeist übers Web koordiniert wird.

Eine exemplarische Betrachtung denkbarer Bedrohungsszenarien kann eine solche reale Gefährdung der nach diesem Schema als „kritisch“ erkannten IT-Systeme belegen und den Eintritt der beschriebenen Entwicklungen als realistisch absichern. Denkbar sind Störungen und Angriffe entlang der materiell-geografischen Struktur des Internets, entlang der softwarebasierten Struktur des Internets, auf die paketvermittelte Kommunikation, auf die Routinginfrastruktur, auf das Domain Name System und auf die Sicherheits- und Zertifikatsinfrastruktur – selbst bis hinein in geschlossene Systeme außerhalb des öffentlichen Internets. Angesichts der Abhängigkeit von diesen Grundelementen der Internetkommunikation, selbst in Fällen, in denen – wie bspw. in der öffentlichen Verwaltung – versucht wird, auf autarke Systeme zu setzen, lassen sich die Auswirkungen auf den Gesundheits- und Energiesektor, die öffentliche Verwaltung im Allgemeinen, sowie den Katastrophenschutz im Speziellen exemplifizieren.

Diese Analyse zwingt dazu, sich vermehrt sowohl technischen, rechtlichen und organisationalen Reaktions- und Abwehrstrategien zuzuwenden. Diese werden im letzten Teil konzipiert, können aber nur als erste Diskussionsanregung verstanden werden:

Während rechtliche Reaktionen, die zwischen Maßnahmen hinsichtlich der „anderen“ kritischen Infrastrukturen, hinsichtlich der IT-Sicherheit anderer kritischer Infrastrukturen und „des Internets“ und der IT-Sicherheit der kritischen IT-Systeme differenziert werden können, sowie technische Maßnahmen der Prävention, Detektion und Reaktion schon diskutiert werden, sind die erforderlichen Veränderungen der Organisationskultur bisher wenig betrachtet. Im Mittelpunkt weiterführender Forschung könnten dabei u. a. Aspekte wie organisationale Achtsamkeit als not-

wendige Voraussetzung für den Schutz kritischer IT-Infrastrukturen und die Herausforderungen der IT-Integration aus organisationaler Sicht stehen.

Jeweils werden dabei aber die Abhängigkeiten zu rechtlichen Maßnahmen (welche Rechtsvorgaben, bspw. auch in Form von Verwaltungsvorschriften etc., sind geeignet, die Einhaltung der organisationalen Achtsamkeit zu sichern bzw. zu fördern) und zu technischen Maßnahmen zu berücksichtigen sein.

Grundsätzlich müssen die Bedrohungspotentiale, Auswirkungen und mögliche Gegenmaßnahmen für das Internet als kritische Infrastruktur in Zukunft sehr viel intensiver interdisziplinär aus verschiedensten Perspektiven des Staates, der Wirtschaft und der Bevölkerung analysiert werden und zu einem Aktionsplan führen, in dem rechtliche, technische und organisatorische Präventions- und Reaktionsmaßnahmen für die Bereiche übergreifend gebündelt werden.

B. Einleitung

Was wäre, wenn das Internet flächendeckend ausfiele, stunden- oder möglicherweise tagelang? Die vielfältigen Abhängigkeiten von und Verflechtungen innerhalb dieser Technologie lassen besorgniserregende Konsequenzen und Szenarien in den Bereich des Vorstellbaren rücken. Daher erscheint es an der Zeit, die technischen Grundlagen sowie den existierenden Rechtsrahmen näher zu betrachten und anhand dessen Handlungsbedarf aufzuzeigen und Reaktionsmöglichkeiten zu entwickeln. Sog. kritische Infrastrukturen, bei deren Ausfall oder Beeinträchtigung es zu dramatischen Folgen für das Gemeinwohl kommen kann, unterliegen nämlich grundsätzlich einer staatlichen Schutzgewähr.

Moderne Gesellschaften sind zunehmend durch hochintegrierte Systeme gekennzeichnet. Während einige, wie etwa das Stromnetz, die Verkehrsinfrastruktur, das Kommunikationsnetz oder die Wasserversorgung als kritische Infrastrukturen bekannt sind, so ist die Bedeutung der diesen Netzen zugrunde liegenden informationstechnischen Infrastruktur noch immer nicht allen in ihrer Tragweite deutlich. Bereits heute werden diese Systeme weitestgehend über das Internet gesteuert, sodass immer mehr Prozesse und Verfahren in einem Netz aus verschiedensten informationstechnischen (IT-)Systemen erbracht werden. Als Beispiel mag die Bestellung eines Taxis dienen: Nachdem der Standort des Kunden über das GPS-System lokalisiert wurde, überträgt die Anwendung des Smartphones diesen an die Taxileitstelle unter Verwendung des Mobilfunknetzes. Nach Beendigung der Fahrt kann der Kunde dann auch mittels seines Smartphones Zahlungssysteme aktivieren. Während für Endanwender der Nutzen derartig integrierter Systeme im Vordergrund steht, so sind deren Angreifbarkeit und damit die Verletzbarkeit von Gesellschaften insgesamt deutlich gestiegen.

Eine ähnlich hohe Systemintegration lässt sich in Unternehmen und Verwaltungen vorfinden. Immer neue Funktionalitäten und Anwendungen werden in bestehende Systemumgebungen integriert, über neue Schnittstellen werden Kunden oder Bürger in Systeme eingebunden oder aber mobile Hardware unterstützt, die den Zugriff auf organisationsinterne Systeme von unterwegs ermöglicht. Gleichzeitig wachsen die komplexen, sozio-technischen Systeme immer weiter, ohne dass diese so jemals geplant worden wären. Das organische Wachstum solcher Systeme, in denen alte Anwendungen außer Dienst gestellt werden, neue Systeme integriert werden, ältere Systeme aktualisiert werden und neue Funktionen zu bestehenden Systemen hinzukommen, hat zu äußerst komplexen, miteinander verwobenen Systemen geführt, die sich nicht nur durch große Heterogenität und mangelnde Standardisierung auszeichnen, sondern deren Funktionalität von einer systemübergreifenden Perspektive kaum mehr erfasst und geschützt werden kann.

Angesichts der zunehmenden Bedeutung des Internets für Gesellschaft, Individuum, Wirtschaft und Staat soll daher der Blick auf diese Grundbedingung gerichtet werden: Ist das Internet eine kritische Infrastruktur? Welche Konsequenzen sind

mit dieser Einordnung – aus rechtlich-regulatorischer, technischer und organisatorischer Perspektive – verbunden? Die Zuordnung des Internets bzw. des Zugangs zu diesem zur essentialen Grundversorgung in einer technisierten Informationsgesellschaft[1] lassen den Vergleich mit anderen solchen Grundversorgungseinrichtungen nicht völlig aus der Luft gegriffen erscheinen. Als problematisch erweist sich indes, dass wesentliche Teile der Kommunikationsinfrastruktur des Internets von privaten Unternehmen beherrscht werden.

[1] So die zutreffende Bezeichnung durch das Bundesverfassungsgericht, vgl. BVerfGE 125, 175 (224).

C. Begriffsdefinition: Kritische Infrastruktur

Die Qualifikation einer Infrastruktur als „kritisch“ erfordert ebenso wie die Entwicklung weitergehender regulatorischer Ansätze mit Bezugnahme auf „kritische Infrastrukturen“ eine nähere Auseinandersetzung mit den Begrifflichkeiten. Der Begriff der kritischen Infrastruktur setzt sich aus unterschiedlichen überkommenen Termini zusammen, auf die im Folgenden eingegangen werden soll, zeigt aber zugleich bereits erste Ansätze einer Herausbildung als Rechtsbegriff. Letzterer wird ebenfalls näher zu betrachten sein, insbesondere mit Blick auf das ihm im Kontext von IT möglicherweise zugrunde zu legende Verständnis.

I. Infrastrukturen

Ursprünglich bezeichnete der Begriff der „Infrastruktur“ erdgebundene Anlagen, die der Mobilität dienen, bspw. Bahnhöfe und Brücken[2], im englischen Sprachraum wurde er zunächst vorrangig militärisch, bspw. für Kasernen und Radarstationen, verwendet[3]. Später setzte sich ein erweitertes Begriffsverständnis durch, das Infrastruktur definiert als die Gesamtheit der materiellen, institutionellen und personalen Anlagen, Einrichtungen und Gegebenheiten, die den Wirtschaftseinheiten im Rahmen einer arbeitsteiligen Wirtschaft zur Verfügung stehen[4]. Gemeinsam ist diesen Begriffsverständnissen, dass es sich bei der Infrastruktur um langlebige Güter handelt, die eine Vielzahl von Nutzungen ermöglichen[5]. Zu einem Rechtsbegriff konnte sich die Infrastruktur – trotz Verwendung in Rechtsnormen – bisher nicht verdichten[6].

---

2 Dieses Verständnis entstand im französischen Sprachraum um 1875; vgl. *Patig*, IT-Infrastruktur, in: Kurbel u. a. (Hrsg.), Enzyklopädie der Wirtschaftsinformatik, Online-Lexikon; abrufbar unter www.enzyklopaedie-der-wirtschaftsinformatik.de.

3 *Frey*, in: Handwörterbuch der Wirtschaftswissenschaft, Bd. 4, 1988, S. 200 ff.; *v. Laak*, Archiv für Begriffsgeschichte 41 (1999), 280 ff.

4 *Jochimsen*, Theorie der Infrastruktur, 1966, S. 145; vgl. auch *Jochimsen/Gustafsson*, in: Simonis (Hrsg.), Infrastruktur, 1977, S. 38 ff.; *Schulze*, Infrastruktur als politische Aufgabe, 1993, S. 40 ff.; *Scheele*, Privatisierung von Infrastruktur, 1993, S. 18 ff.; s. auch *Willke*, Systemtheorie II, 1994, S. 240: „öffentliche Komplementär- und Supporteinrichtungen“.

5 *Patig* (Fn. 2).

6 Dieses Urteil von *Hermes*, Staatliche Infrastrukturverantwortung, 1998, S. 170 ff., ist wohl weiterhin berechtigt. S. zur Infrastruktur als Rechtsbegriff auch *Sonntag*, IT-Sicherheit kritischer Infrastrukturen, Diss. Münster 2003, S. 29 ff.

II. IT-Infrastruktur/Internet

Unter IT-Infrastrukturen versteht man Hardware[7], einschließlich der Netzanbindungen, Software und bauliche Einrichtungen für die Nutzung von Diensten im Internet und den Betrieb von (Anwendungs-)Software. Auf ihnen baut das Internet auf. Das Internet ist ein Zusammenschluss von Netzen verschiedener Organisationsformen und Eigentümer, um die gegenseitige Erreichbarkeit und Kommunikation weltweit sicherzustellen[8]. Es basiert auf der Nutzung gleicher Kommunikationsprotokolle über eine Reihe von standardisierten Übertragungstechniken. Das Internet verfügt ebenfalls über alle Eigenschaften einer Infrastruktur, da es Staat, Wirtschaft und Gesellschaft systemübergreifend als Handlungsplattform dient. Zudem erscheint es als Prototyp einer Einrichtung, die eine Vielzahl unterschiedlicher Nutzungen ermöglicht – angesichts der Entwicklungen z. B. zum Smart Life, zum Internet der Dinge und des mobilen Internets werden die Nutzungsmöglichkeiten in den nächsten Jahren weiter ansteigen. Vielleicht handelt es sich beim Internet (bzw. den Infrastrukturen, auf denen dieses basiert) um *die* entscheidende Infrastruktur der nächsten Jahrzehnte.

III. Kritische Infrastruktur

Mit dem Begriff der „kritischen Infrastruktur“ werden Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen umschrieben, bei deren Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe bis hin zu Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten können[9]. Einengende oder erweiternde Auslegungen können dabei zum einen am Begriffsmerkmal der „Organisationen und Einrichtungen“ ansetzen, die in einem weiten Verständnis auch Dienste, Prozesse und Systeme erfassen können. Zum anderen kann bei der erforderlichen Gefährdungslage angesetzt werden: diese lässt sich eng auf das Erfordernis einer Gefahr für die öffentliche Sicherheit begrenzen, denkbar ist aber auch eine Ausdehnung auf andere „Schäden für das Gemeinwesen, für Wirtschaft und Bevölkerung“[10].

---

7 Hierzu gehören bspw. Rechentechnik (Computer, Storage-Systeme), Netzwerktechnik (Switches, Kabel), Peripheriegeräte (Tastatur, Belegleser, Bildschirm, Drucker, Scanner) sowie Geräte zum Betrieb der Hardware (Racks, unterbrechungsfreie Stromversorgung).

8 Näher dazu unten unter Gliederungspunkt D.

9 So die Definition des *Bundesministerium des Innern,* Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), 2009, S. 4.

10 *Schmidt-Preuss*, in: Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen: IT und Energie, 2010, S. 79 ff.; vgl. Art. 2a der Richtlinie des Rates über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern (2008/114/EG) v. 8. 12. 2008, ABl EG Nr. L 345 v. 23. 12. 2008, S. 75.

In jeden Fall ist unerheblich, ob die Infrastruktur privat oder öffentlich betrieben wird[11]. Etwa 80 % der kritischen Infrastrukturen in Deutschland befinden sich in privater Hand[12], 20 % sind dem öffentlich-rechtlichen Sektor zuzuordnen. Die Aufgabe des Schutzes kritischer Infrastrukturen stellt sich trotz der unterschiedlichen Verteilung für Staat und für private Unternehmen in gleicher Weise und führt zu einer faktischen Verantwortungsteilung[13], ohne dass damit allerdings etwas über die rechtliche Zuordnung ausgesagt ist. Aus der Aufteilung wird aber deutlich, dass im Hinblick auf Sicherheitsvorkehrungen nicht alleine der Staat, sondern maßgeblich auch der privatwirtschaftliche Sektor gefordert ist[14].

IV. Rechtsbegriff „Kritische Infrastruktur“

Der Begriff der kritischen Infrastruktur wurde gesetzlich erstmals in der Neufassung des Raumordnungsgesetzes (ROG)[15], die zum 1. 1. 2009 in Kraft trat, niedergelegt. Die Gesetzesbegründung verwendet die Definition des Bundesministeriums des Innern[16] und sieht die kritischen Infrastrukturen insbesondere durch vorsätzliches Handeln (Terror, Krieg), menschliches oder technisches Versagen sowie Naturereignisse bedroht[17]. Dass als Beispiel für die Berücksichtigung im Zuge der Raumordnung eine parallele Trassenführung unterschiedlicher Infrastrukturen als bedenklich angesehen wird[18], deutet bereits auf ein leitungs-/netzbezogenes Infrastrukturverständnis hin. Grundsätzlich wird unter Infrastruktur nach wie vor die Versorgung von Bevölkerung und Unternehmen mit Energie- und Transportdienstleistungen, Trinkwasser, Einrichtungen des Gesundheits- und des allgemeinen Ver- und Entsorgungswesens verstanden. Als Rechtsbegriff findet sich die „kritische Infrastruktur“ neben § 2 ROG zudem bspw. in § 3 BSIG[19], den §§ 17, 18 ZSKG[20] sowie prominent im Entwurf für ein IT-Sicherheitsgesetz[21] (im Folgenden: IT-SIG-E), auf den später einzugehen sein wird.

---

11 *Möllers/Pflug*, in: Kloepfer (Fn. 10), S. 47 (52).

12 *Schäuble*, in: Kloepfer (Fn. 10), S. 21 (24).

13 *Kloepfer*, in: ders. (Fn. 10), S. 9 (17).

14 *Gaycken/Karger*, MMR 2011, 3 (5 f.).

15 Raumordnungsgesetz vom 22. 12. 2008, BGBl. I S. 2986.

16 Oben Fn. 9.

17 BT-Drs. 16/10292, S. 21.

18 Ebd.

19 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik vom 14. 8. 2009, BGBl. I S. 2821.

20 Gesetz über den Zivilschutz und die Katastrophenhilfe des Bundes vom 25. 3. 1997, BGBl. I S. 726.

21 Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Referentenentwurf, Stand: 5. 3. 2013), abrufbar unter www.bmi.bund.de.

V. Erweitertes Verständnis im Kontext der IT-Abhängigkeit

Aufgrund der mit den digitalen Informations- und Kommunikationstechniken zunehmenden Überschneidungen zwischen den verschiedenen technischen und sozialen Infrastrukturbereichen rückt verstärkt – auch europäisch veranlasst – die Kommunikationsinfrastruktur in den Fokus der Betrachtung. Denn auch die Funktionsfähigkeit der Bereiche Transport und Verkehr, Energie, Gefahrstoffe, Finanz-, Geld- und Versicherungswesen, Versorgung, Verwaltung und Justiz, aber auch sonstiger Bereiche wie Bildung, Forschung und Medien hängt zunehmend vom Funktionieren und der Zuverlässigkeit der Informationstechnik ab[22]. So hat sich das Europäische Parlament am 12. 6. 2012 in einer Entschließung über den Schutz kritischer Informationsstrukturen[23] dafür ausgesprochen, dass Besitzer und Betreiber kritischer Informationsstrukturen Anwender in die Lage versetzen und dabei unterstützen sollen, sich vor bösartigen Angriffen und/oder Störungen zu schützen. Schon im Dezember 2006 legte die Kommission eine Mitteilung mit einem allgemeinen Rahmen für Aktivitäten zum Schutz kritischer Infrastrukturen auf EU-Ebene vor[24], die mit der Richtlinie 2008/114/EG über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern[25], konkretisiert wurde. In Deutschland wurde diese bspw. durch § 12g EnWG umgesetzt. 2009 legte die Kommission dann eine Mitteilung über den „Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität“[26] vor, in der ein Aktionsplan zum Schutz kritischer Informationsinfrastrukturen auf nationaler und Unionsebene enthalten ist. Eine Schlüsselrolle soll der 2004 gegründeten EU-Agentur für die Netz- und Informationssicherheit (ENISA) zukommen. Die Kommission soll eine Strategie vorlegen, die Grundsätze, Ziele, Methoden, Instrumente und Richtlinien angibt, die erforderlich sind, um die nationalen und EU-weiten Bemühungen zur Sicherstellung eines sicheren, dauerhaften, robusten und zuverlässigen Dienstes zu vereinheitlichen.

Diese Verlagerung des Schwerpunktes der Betrachtungen im Bereich kritischer Infrastrukturen, weg von physischen Infrastrukturen und deren realem Schutz hin

---

22 *Spannowsky*, in: ders./Runkel/Goppel (Hrsg.), Raumordnungsgesetz, 2010, § 2 Rn. 89.

23 Entschließung des Europäischen Parlaments vom 12. 6. 2012 zu dem Schutz kritischer Informationsinfrastrukturen, P7_TA(2012)0237.

24 Mitteilung der Kommission über ein europäisches Programm für den Schutz kritischer Infrastrukturen, KOM (2006) 786 endg. vom 12. 12. 2006.

25 Oben Fn. 10.

26 Mitteilung der Kommission über den Schutz kritischer Informationsinfrastrukturen „Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität“ KOM (2009) 149 endg. vom 30. 3. 2009.

zu den technischen Kommunikationsgrundlagen dieser Dienste, zeigt die besondere Rolle der „IT“. Sie nimmt nämlich eine „Doppelfunktion“ ein; einerseits wird die IT – eigentlich ist oft „das Internet“ gemeint – selbst als kritische Infrastruktur eingestuft, andererseits sind IT und Internet Funktionsbedingung zahlreicher anderer kritischer Infrastrukturen.

D. Gegenstand der Betrachtung: IT, IKT, Internet, Netze

Zur Sicherstellung der technischen Beherrschbarkeit werden komplexe Systeme strukturiert entworfen und aufgebaut. In diesem Kapitel werden grundlegende Strukturen des Internets kurz dargestellt, um Begriffe zu definieren und eine Basis für die anschließende Analyse zu schaffen.

Das Internet ist ein Zusammenschluss von Netzen verschiedener Organisationsformen und Eigentümer, um die gegenseitige Erreichbarkeit und Kommunikation weltweit sicherzustellen. Es basiert auf der Nutzung gleicher Kommunikationsprotokolle über eine Reihe von standardisierten Übertragungstechniken.

I. Begriffsdefinition „Internet“ und Netze

Durch die Zusammenschaltung von Netzwerken unter unterschiedlicher administrativer Verwaltung entsteht ein weltweites Netz zum Austausch von Daten, in dem prinzipiell jeder Rechner mit einem anderen Rechner Daten austauschen kann, sofern es nicht aus Sicherheitsgründen oder aufgrund der Adressknappheit[27] beim Internet Protocol Version 4 (IPv4) zu Einschränkungen kommt.

Im Gegensatz dazu steht der Begriff Intranet für ein internes Netz, das sich unter vollständiger administrativer Kontrolle des Netzbetreibers (bspw. eines Unternehmens) befindet. Meist werden Zugriffe aus anderen Netzen (wie dem Internet) durch Sicherheitsanwendungen (bspw. Firewalls oder Sicherheits-Gateways) verhindert oder nur aufgrund spezieller Regeln zugelassen[28].

Davon zu unterscheiden ist die Verwendung von Internettechnologien und Internetprotokollen, in geschlossenen Netzen, die keinen Zugang zu anderen Netzen bieten. Der Vorteil liegt dabei in der Verfügbarkeit vergleichsweise preiswerter und leistungsfähiger Hard- und Softwarekomponenten. Aus diesem Grund ist die Entwicklung zu erkennen, dass sich die Internet-Technologie und die IP-Protokollfamilie in immer mehr Gebieten durchsetzen, entweder weil die durchgängige Vernetzung erreicht werden soll oder weil die Verwendung etablierter Standards und Komponenten wirtschaftliche Vorteile verspricht.

---

[27] Mittels Mechanismen wie NAT (Network Address Translation) oder CGN (Carrier-grade NAT) können auch Endgeräte ohne öffentliche IP-Adresse weltweit kommunizieren, allerdings können diese nur eingeschränkt aus dem Internet erreicht werden.

[28] Vgl. die Definitionen des Bundesamts für Sicherheit in der Informationstechnik, z. B. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html.

II. Technische Strukturierungsmerkmale des Internets

1. Gliederung in Protokollschichten

Zur Datenübertragung und Steuerung der Kommunikation sind Protokolle notwendig, die nach Schichten (engl. „Layer“) strukturiert werden. Die verschiedenen Protokollschichten übernehmen dabei spezifische Aufgaben und erlauben eine Abstraktion beim Zugriff auf die Funktionalität. Das TCP/IP-Referenzmodell umfasst vier Schichten: Netzzugang, Internet, Transport, Anwendung[29].

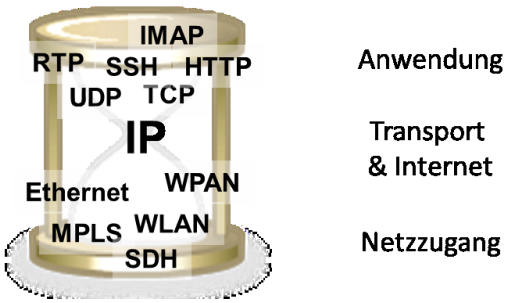


ABBILDUNG 1: SANDUHR-MODELL DES INTERNETS UND PROTOKOLLSCHICHTEN

Zur Veranschaulichung dient das „Sanduhr-Modell“ des Internets: Die Internet-Protokollschicht mit dem IP-Protokoll ist der gemeinsame Nenner aller Kommunikation und sorgt für die prinzipiell mögliche durchgängige Kommunikation zwischen vielen Endgeräten und Netzen. Unterhalb des IP-Protokolls wird der Netzzugang durch Einsatz verschiedenster Technologien, wie bspw. Ethernet oder WLAN, an das jeweilige Nutzungsszenario angepasst. Oberhalb der Transportschicht[30] kommen verschiedenste und vielfältige Anwendungsprotokolle zum Einsatz, wie das bekannte HTTP-Protokoll zur Übertragung von Webinhalten.

An diesem Modell wird die zentrale Rolle des Internet-Protokolls erkennbar und welche Rolle es für die durchgängige Kommunikation spielt. Das IP-Protokoll sorgt insbesondere für die globale Adressierung aller Teilnehmer.

Weiterhin soll darauf hingewiesen werden, dass das Web nur eine Anwendung auf Basis von Internet-Protokollen ist, andere Anwendungen wie E-Mail oder Telefonie

---

29 http://de.wikipedia.org/wiki/Internetprotokollfamilie.

30 Auf der Transportschicht werden normalerweise die Protokolle TCP und UDP verwendet, einzelne weitere Protokolle sind im Einsatz. Für diese Betrachtung kann vereinfacht vom „TCP/IP“-Bild ausgegangen werden und die Internet- und die Transportschicht gemeinsam betrachtet werden.

nutzen andere Anwendungsprotokolle. Die gelegentliche Gleichsetzung von Internet und Web ist irreführend.

2. Topologie des Internets

Das Internet als Zusammenschluss von Netzen unter verschiedener administrativer Verwaltung ist eine heterogene Struktur. Vereinfacht können Zugangsnetze (Access Networks) und Kernnetze (Backbones) unterschieden werden.

Zugangsnetze verbinden einzelne Geräte (z. B. beim Mobilfunk) oder lokale Netze (z. B. Firmennetze) mit dem Internet. Dabei kommen verschiedenste Technologien zum Einsatz. In Deutschland sind DSL oder Kabelanschluss für den Internet-Zugang von Privathaushalten oder kleineren Unternehmen verbreitet. Hinzu kommen Mobilfunk und WLAN, hauptsächlich für mobile Geräte. Genauso ist über den mobilen Zugang aber auch der Anschluss von Heimnetzen möglich, insbesondere in ländlichen Gebieten[31]. Eine weitere wichtige Technologie sind Glasfaserverbindungen, die im Anschlussbereich für den Zugang von Firmen und anderen Organisationen eine wichtige Rolle spielen. Zugangsnetze werden von Netzbetreibern bzw. Mobilfunkbetreibern betrieben und der Internetzugang als Dienst über Telekommunikationsanbieter (z. B. Internet-Provider oder Mobilfunkprovider) angeboten[32]. Die Leistungsmerkmale eines Dienstes wie dem Internetzugang werden in Service Level Agreements (SLA) beschrieben und umfassen bspw. Angaben zu verfügbaren Bandbreiten, Datenvolumen oder der Verfügbarkeit des Anschlusses.

Die verschiedenen Kernnetze der Telekommunikationsunternehmen basieren vorwiegend auf Glasfaserinfrastrukturen. Diese Netzinfrastruktur wird entweder direkt genutzt oder es werden auf dieser Basis Transportnetze realisiert (bspw. als MPLS-Netz). In beiden Fällen werden die Kommunikationsverbindungen in Bezug auf ihre Leistungsfähigkeit überwacht und z. B. bei Ausfall ein Alarm ausgelöst und ggf. automatisch entsprechender Ersatz geschaltet. Die Nutzung von Transportnetzen ermöglicht eine feinere Steuerung der Datenflüsse über das Kernnetz (Traffic Engineering), vor allem in Bezug auf die Bereitstellung kleinerer Datenraten bzw. die Sicherstellung von Qualitätsmerkmalen bei der Datenübertragung.

Auf Basis von Glasfaserinfrastrukturen oder von Transportnetzen werden grundsätzlich drei Arten von Transportdiensten realisiert:

---

[31] Informationen über die Breitbandversorgung von Privathaushalten mit Karten zur Abdeckung und der Verfügbarkeit von Technologien enthält der Breitbandatlas unter http://www.zukunft-breitband.de/DE/breitbandatlas.html.

[32] Es gibt grundsätzlich zwei Arten von Internet-Providern (Access Provider): entweder wird der Internetzugang auf eigenen Netzen angeboten oder auf Basis von fremden Netzen.

- Interne Transportdienste für Sprache, Video oder bspw. die Kopplung von Rechenzentren (Cloud-Infrastrukturen), insbesondere zur Sicherstellung der Dienstqualität bei effizientem Transport und Management der Verbindungen.
- Virtuelle private Netze für Firmenkunden, die auf Basis der gleichen Glasfaserinfrastrukturen bzw. Transportnetze eine völlige Trennung zum Internet darstellen.
- Transport des öffentlichen Internet-Verkehrs.

Bei dieser Gegenüberstellung wird klar, dass Telekommunikationsunternehmen oder Internet-Dienstleister über eigene Infrastrukturen verfügen, die allenfalls mittelbar dem öffentlichen Internet zugerechnet werden können. Diese Infrastrukturen werden bspw. intern in Produkten zur Sicherstellung der Dienstqualität eingesetzt oder auch anderen Organisationen zum Aufbau vom Internet getrennter, privater Netze angeboten.

Im Internet-Modell gibt es keine zentrale Steuerung von Netzen oder Kommunikationsverbindungen. Wenn ein Kommunikationsteilnehmer nicht im Netz des gleichen administrativen Bereichs ist, werden daher die Datenpakete in Richtung des Empfängers in andere Netze weitergeleitet. Dabei kann der Datenverkehr über weitere, dazwischen liegende Kernnetze übertragen werden oder direkt in ein Netz übergehen, in dessen administrativer Hoheit auch der Empfänger zu finden ist[33]. Die Zusammenschlüsse von Netzen basieren auf zwei Prinzipien: Einerseits können Netze über normale Netzzugänge vergleichbar einem Kundenanschluss zusammengeschaltet werden oder es findet ein Austausch auf Basis von Gegenseitigkeit statt (Peering). Im Fall des Zusammenschlusses über Netzzugänge steht normalerweise der finanzielle Ausgleich im Vordergrund. Bspw. kann ein lokaler ISP seinen Kunden einen Internetzugang anbieten und die dafür benötigte Konnektivität zum Internet von einem Betreiber eines Kernnetzes einkaufen. Verschiedene Provider können aber auch an Austauschknoten (Internet Exchange Point) ihren Internetverkehr auf dem Prinzip von Gegenseitigkeit austauschen, um dem Grundsatz des Netzwerkprinzips zu entsprechen[34].

3. Technische Eigenschaften/Komponenten des Internets

Nach der ersten Übersicht über die Strukturmerkmale des Internets und von Internetprotokollen soll auf einige für diese Untersuchung relevante technische Eigenschaften näher eingegangen werden.

---

[33] Vgl. hierzu die Klassifizierung von Internet-Providern in „tier“-Klassen, bspw. in http://en.wikipedia.org/wiki/Tier_1_network.

[34] Nach dem Netzwerkprinzip steigt der Nutzen des Netzes mit der Anzahl der Teilnehmer.

Eigenschaften des IP-Protokolls

Die technische Realisierung der Datenübertragung erfolgt auf Basis des IP-Protokolls. Die Kommunikation auf der IP-Schicht erfolgt paketvermittelt, d. h. die Daten höherer Protokollschichten und letztlich der Anwendungen werden in Datenpakete zerlegt und mit einem Protokollheader versehen, der die notwendigen Informationen zur Übertragung enthält (hauptsächlich Start- und Zieladresse, Bezeichnung des logisch darüber liegenden Protokolls. Auf der IP-Schicht ist die Übertragung verbindungslos, d. h. es gibt vom Netz keine Garantie, dass einzelne IP-Pakete einer Anwendung gleichartig behandelt werden[35].

Für viele Protokolle und Anwendungen gilt das Ende-zu-Ende-Prinzip, bei dem die Steuerung der Kommunikation durch die Endgeräte erfolgt und das dazwischen liegende Netz vergleichsweise einfach aufgebaut sein kann. Die Endgeräte stellen auch die dienstspezifischen Kommunikationsfunktionen zur Verfügung, d. h. sie verfügen über den gleichen Internet-Anschluss, erbringen aber so unterschiedliche Dienste wie die Übertragung von Web-Inhalten oder Telefonie.

Die Steuerung der Kommunikation erfolgt als sog. Nutzkanal-Signalisierung (in-band signalling) über die gleichen Wege wie die Übertragung der Nutzdaten, d. h. die Steuerung der Kommunikation ist prinzipiell für jeden Nutzer eines Netzes zugänglich. Aus diesem Grund muss die Steuerung der Kommunikation besonders geschützt werden.

Routing

IP-Pakete enthalten Quell- und Zieladresse, anhand derer sie durch die Netze geleitet werden. Netze werden über Router miteinander verbunden, die über die Wegewahl entscheiden. In Routingtabellen ist festgehalten, welche Netzbereiche über welchen Pfad erreicht werden können. In einem streng hierarchisch organisierten Gesamtnetz kann die Wegewahl sich zunächst an größeren, zusammenhängenden Netzbereichen orientieren und dann innerhalb dieses Bereiches nahe dem Zielnetz weiter verfeinert werden, was das Routing übersichtlich und die Routingtabellen optimal klein halten würde. Aufgrund des weltweiten Internet-Wachstums und bspw. der vermehrten Nutzung von redundanten Netzanbindungen über mehrere Internet Service Provider müssen viele Netze im großen Umfang in den Routern des Internets bekannt sein, was zu großen Routingtabellen führt.

Routingprotokolle sorgen dafür, dass die Information über die Erreichbarkeit von Netzbereichen zwischen den Routern ausgetauscht wird und sich somit die Netz-

[35] Diese grundsätzliche Betrachtung gilt hauptsächlich für die Ende-zu-Ende-Kommunikation über das Internet. Einzelne Netzkomponenten sind sehr wohl in der Lage, gleichartige Paketströme (Flows) zu behandeln und es sind auch Protokollmechanismen zur Erreichung von Dienstqualität (QoS) definiert.

konfiguration dynamisch ändern kann. Da die Kommunikation im Internet über das IP-Protokoll verbindungslos funktioniert, können IP-Pakete weitergeleitet werden, ohne die Sicherheit, dass sich in Richtung der Weiterleitung wirklich der Empfänger befindet. Es muss also nicht unbedingt eine „Gegenstelle" direkt erreichbar sein, um eine Routingentscheidung zu treffen. Das macht das Internet einerseits robust und skalierbar, kann aber auch dazu führen, dass Netze vom Internet aus ohne aussagekräftige Fehlermeldung nicht mehr erreichbar sind, wenn es zu Routingfehlern kommt.

Domain Name System (DNS)

Die Adressierung und das Routing basieren auf den in IP-Paketen enthaltenen IP-Adressen (z. B. 192.0.2.123 für IPv4 oder 2001:db8::123 für IPv6). Da diese technischen Adressen für Menschen schwer handhabbar sind, wurde das Domain Name System eingeführt, das auf textuellen Bezeichnern basiert (z. B. www.example.org).

DNS basiert auf einer Baumstruktur, in der die Namen von rechts aufgelöst werden. Im obigen Beispiel ist „org" die Top Level Domain, innerhalb derer die Domain „example" festgelegt ist. Komplettiert wird die Adresse eines Internet-Endgeräts durch den Hostnamen „www", der wiederum innerhalb der Domain festgelegt ist und auf eine IP-Adresse verweist.

Die Verwaltung der Namensräume unterliegt sog. Registraren, für die Top Level Domain „.de" ist das bspw. die DENIC eG[36]. Die reine Datenübertragung im Internet funktioniert technisch auch ohne das DNS, allerdings wären dann Ressourcen nicht oder nur schwer auffindbar. Technisch erfolgt der Zugang zu einem sog. Nameserver meist über den Internet Service Provider, aber auch bspw. Google betreibt einen bekannten öffentlichen Nameserver (IPv4-Adresse: 8.8.8.8)[37]. Daneben existieren verschiedene unabhängige DNS-Strukturen, die praktisch aber wenig Bedeutung haben[38]. Sie sind meist politisch motiviert, bspw. mit dem Anspruch, Zensurmaßnahmen zu umgehen oder der (früher stärkeren) US-Dominanz beim Betrieb des DNS entgegen zu wirken.

Mittels des DNS kann zudem die Zuordnung zwischen Rechnernamen und IP-Adressen flexibilisiert werden. Ein Rechner kann verschiedene Namen bekommen, die aber immer auf die gleiche IP-Adresse verweisen (z. B. können neben dem Rechnernamen zusätzlich virtuelle Funktionsnamen vergeben werden, wie „www" oder „mail"). Oder der gleiche DNS-Name kann auf verschiedene konkrete Rechner verweisen (z. B. zur Lastverteilung: Angesprochen wird immer www.example.org,

---

36 http://www.denic.de.

37 https://developers.google.com/speed/public-dns/?hl=de.

38 Als Beispiel: OpenNIC, http://www.opennicproject.org/.

aber je nach Region oder Auslastung werden verschiedene konkrete Rechner adressiert).

Integrierte Plattformen

Das Internet entwickelte sich auf Basis der bisher geschilderten Mechanismen. Zur Verbesserung der Leistungsfähigkeit einzelner Dienste kommen Plattformen zum Einsatz, die sich im Idealfall transparent gegenüber bestehender Infrastruktur und den Endgeräten verhalten. Das Ende-zu-Ende-Prinzip des Internets führt dazu, dass neue Anwendungen sehr schnell und unabhängig von der bestehenden Infrastruktur eingeführt werden können. Sollen aber Mechanismen mit Auswirkungen auf die Netzkomponenten entlang des Kommunikationspfads eingeführt werden, so ist das bei der transnationalen Struktur des Internet nur sehr langsam bzw. evolutionär möglich. Aus diesem Grund werden verschiedene Mechanismen unterhalb und oberhalb der Internet-Protokollschicht eingesetzt, um das Verhalten von Internetdiensten zu beeinflussen. Ein Beispiel ist das schon genannte Traffic Engineering, mit dem die Netzinfrastruktur zur Übertragung von IP-Paketen unter Effizienz oder Qualitätsgesichtspunkten optimiert wird.

Ein weiteres Beispiel sind Content Delivery Networks (CDN). Zur effizienten Bereitstellung bspw. von Multimediainhalten werden Anfragen von Endgeräten bei vielen Diensten nicht von einer zentralen Serverfarm direkt verteilt, sondern diese Anfragen werden von einem CDN beantwortet. Dabei handelt es sich um topologisch verteilte Server, die bspw. über Backbones in verschiedenen Regionen der Welt gut erreicht werden können. Die ursprünglichen Inhalte werden innerhalb des CDN repliziert und verteilt, damit der Zugriff vom Benutzer effizienter und schneller über kürzere Wege erfolgen kann. Der Mechanismus zum Zugriff auf die verteilten Server kann bspw. über DNS realisiert sein, wobei in diesem Fall der Zugriff auf den gleichen DNS-Namen in verschiedene Serveradressen aufgelöst wird.

Weitere Plattformen, die in diesem Zusammenhang genannt werden sollen, sind die Dienstplattformen von großen Diensteanbietern wie Google oder Facebook. Im engeren Sinne stellen sie Dienste auf Basis des Internets bereit und sind also selber kein Teil der Internet-Infrastruktur. Allerdings bieten sie auch Teilfunktionen, auf die sich ggf. andere Dienste abstützen, wie bspw. die Benutzeridentifikation, und sind daher ggf. bei einer Gesamtbetrachtung zu berücksichtigen.

E. Das Internet als kritische Infrastruktur?!

Die vielfältigen technischen Verflechtungen veranlassen schnell dazu, „dem Internet“ auch den Stempel der „kritischen Infrastruktur“ aufzudrücken. In diesem Kontext bedarf es aber einer begrifflichen und damit auch inhaltlichen Einschränkung: pauschale Zuordnungen mögen plakativ sein, als Grundlage konkreter Maßnahmen sind sie nicht geeignet. Wie § 12g EnWG exemplarisch für den Energiesektor zeigt, ist nicht die gesamte „Energieversorgung“, der gesamte „Energiesektor“ als solcher als kritische Infrastruktur einzustufen, sondern nur – im europäischen Kontext – diejenigen Anlagen oder Teile von Anlagen des Übertragungsnetzes, deren Störung oder Zerstörung erhebliche Auswirkungen in mindestens zwei Mitgliedstaaten der Europäischen Union haben kann. Was bedeutet dies für das Internet als kritische Infrastruktur? Vergegenwärtigt man sich die (technische) Funktionsweise des Internets, die verschiedene Ebenen der Internet-Nutzung und schließlich die Differenzierung von „IT“ und „Internet“, lassen sich die Konturen schärfen.

I. Funktionsweise und daraus resultierende Einschränkungen

Die differenzierte Betrachtung der technischen Eigenschaften des Internets hat gezeigt, dass neben physikalischen Elementen auch bestimmte Dienste zur Funktionsfähigkeit des Netzes notwendig sind, bspw. die DNS-Server, deren Hauptaufgabe die Beantwortung von Anfragen zur Namensauflösung ist. Davon zu unterscheiden sind Anwendungen, die nicht der Funktionsfähigkeit des Internets dienen, sondern auf dieser Infrastruktur bestimmte Funktionalitäten bereitstellen (E-Mail u. a.).

Damit wird zunächst deutlich, dass wesentliche Elemente der Infrastruktur, die als „kritisch“ eingestuft werden könnten, „Telekommunikationsinfrastrukturen“ im ganz herkömmlichen Sinne sind, die schon seit jeher den kritischen Infrastrukturen zugeordnet werden. Nicht jeder „Netzteil“, jedes „Teilnetz“ und jede Einrichtung, die auch zur flächendeckenden Funktionsfähigkeit des Internets bzw. der Versorgung des letzten Teilnehmers in einem bayerischen Bergdorf beiträgt, ist auch zugleich kritisch. Ein Router bzw. Switch, der eine Kleinstadt versorgt, mag die Erheblichkeitsschwelle, die „Systemrelevanz“[39], nicht erfüllen, der DE-CIX in Frankfurt, als größter deutscher Netzknoten- und Datenaustauschpunkt[40], und verschiedene Backbone-Netze (wie etwa das der Deutschen Telekom) vielleicht schon eher. Im europäischen Kontext wäre auch hier – vergleichbar dem Energiesektor – eine Beschränkung auf diejenigen Elemente der Telekommunikationsinfrastruktur

---

[39] Dieser Terminus ist der Diskussion um die „Bankenrettung“ entlehnt, erscheint aber auch im Kontext kritischer Infrastrukturen passend.

[40] Zu dessen Aufbau s. noch unten Gliederungspunkt F. I. 1.

denkbar, deren Ausfall sich in mehreren Mitgliedstaaten auswirkt. Dennoch bleibt zu berücksichtigen, dass sich „das Internet“ und seine Funktionsfähigkeit nicht in Telekommunikationsinfrastrukturen erschöpfen, es vielmehr ein „Delta“ verbleibt, welches nicht vom TKG, aber auch von anderen Regulierungen nicht erfasst wird (Beispiel: DNS-Server). Die Besonderheit des Internets besteht gerade darin, dass nicht eine Entität „Gesamtverantwortung“ für das Gesamtsystem trägt, sondern die Verantwortlichkeit auf viele Akteure verteilt ist. Insofern ist anzuerkennen, dass sich kaum alle Teilbereiche und -aspekte werden regulieren lassen, sodass ggf. andere Maßnahmen ergänzend hinzutreten müssen (bspw. resiliente Systeme durch Entnetzung)[41].

II. Zugangsebenen und daraus resultierende Einschränkungen

Wie auch in anderem Kontext – nämlich bei der Frage, ob den Staat eine Gewährleistungspflicht trifft, den Zugang zum Netz aufgrund der individuellen Bedeutung für jeden Einzelnen abzusichern (Recht auf Internet[42]) – muss zwischen den verschiedenen Ebenen, aus denen „das Internet“ besteht bzw. aus denen die Nutzbarkeit des Internets für Unternehmen, Behörden und jeden Einzelnen folgt, differenziert werden: 1. die Bereitstellung einer übergreifenden (Telekommunikations-) Infrastruktur, die einen Zugang zum Internet gewährleisten kann, 2. muss der Einzelne auch über individuelle Infrastrukturkomponenten verfügen, die einen Zugang ermöglichen, und 3. bedarf er auch eines solchen individuellen Zugangs, im Sinne einer privatrechtlichen Vereinbarung mit einem Provider, die die konkrete Nutzung sicherstellen kann.

Offensichtlich ist, dass ohne eine übergreifende Telekommunikationsinfrastruktur jegliche Internetnutzung von vornherein ausgeschlossen ist. Die Versorgung mit leitungsgebundenen oder Funknetzen ist Teilelement des Rechts auf Internet – die Breitbanddebatte der letzen Jahre hat dies deutlich gezeigt. Sie illustriert auch, dass in diesem Bereich die staatliche oder staatlich initiierte Bereitstellung durch Private den Schwerpunkt bilden muss – niemand kann auf sich allein gestellt für diese Infrastrukturen sorgen. Die übergreifende Infrastruktur bzw. die darauf bezogene Gewährleistungspflicht (verfassungsrechtlich in Art. 87f GG angelegt) beinhaltet zunächst zwei Komponenten: einerseits Aufbau, Pflege und Betrieb der Netzinfrastrukturen, andererseits aber auch nachgelagert die Erbringung von Diensten auf den Netzen, ohne welche die Infrastruktur für den Einzelnen ohne Nutzen bliebe. Und im hier relevanten Kontext: die Absicherung der kritischen, systemrelevanten Teile dieser Infrastruktur – der Aufbau einer ungesicherten Infrastruktur erfüllt

---

41 *Schulz/Tischer,* ZG 2013, 339 (350).

42 Ausführlich *v. Lewinski*, RW 2011, 70 ff.; *Luch/Schulz* Das Recht auf Internet als Grundlage der Online-Grundrechte, 2013.

die Gewährleistungsverantwortung allenfalls rudimentär. Im Fall der Fälle bliebe sie aber nutzlos. Insofern ist davon auszugehen, dass der verfassungsrechtliche Grundversorgungsauftrag auch zu angemessenen Sicherheitsvorkehrungen des Staates bzw. zur Verpflichtung der privaten Betreiber auf solche Maßnahmen zwingt[43]. Damit wird IT-Sicherheit zum Element der (E-)Daseinsvorsorge[44]. Deren übrige Bestandteile, namentlich die Absicherung eines persönlichen Zugangs durch individuelle Infrastrukturkomponenten, entbehren allerdings, anders als die übergreifende Infrastruktur, dem Merkmal der Kritikalität.

III. Verhältnis von Internet und IT zu anderen kritischen Infrastrukturen

Abschließend ist noch das Verhältnis von Internet und IT zueinander sowie zu anderen kritischen Infrastrukturen zu beleuchten. Hier bedarf es einer differenzierenden Sichtweise: IT als solche kann keine kritische Infrastruktur darstellen – sie ist allenfalls Mittel zum Zweck, niemals Selbstzweck. Insofern ist immer nur diejenige IT „kritisch" im hier relevanten Maßstab, die auch für eine andere kritische Infrastruktur zwingend erforderlich ist. Dies gilt bspw. für Steuerungseinrichtungen von Verkehrs-, Energie-, Entsorgungs- und Gesundheitsinfrastrukturen. Soweit derartige Organisationen und Einrichtungen, die aus ihrem Zweck, ihrer Funktion und ihrer Bedeutung heraus als kritische Infrastruktur zu bewerten sind, auch auf das „Internet" angewiesen sind, strahlt die Bedeutung dann auch auf dieses aus. Derartige Konstellationen sind bspw. im Bereich der öffentlichen Verwaltung (die zumindest in Teilen auch als kritische Infrastruktur einzuordnen ist – bspw. Polizei- und andere Sicherheitsbehörden) denkbar, wenn sich die Aufgabenerfüllung, wenn auch „getunnelt", dennoch über öffentliche Telekommunikationsleitungen, im Sinne des Internets, vollzieht. Diese – wahrscheinlich weitgehend geteilte – Einschätzung, dass Sektoren existieren, für die das Internet eine größere Bedeutung besitzt (nämlich die kritischen Infrastrukturen) als in anderen Bereichen, birgt zugleich aber erheblichen politischen Diskussionsbedarf. In dieser Bewertung liegt nämlich ein Angriff auf die so oft hochgehaltene Netzneutralität: kommt der Aufbau eigener Netze für bestimmte kritische Infrastrukturen, bspw. das Gesundheitswesen, aus verschiedenen Gründen nicht in Betracht, bleibt nur die Absicherung des „Sonderbedarfs" an Netzzugang und Netznutzung durch „Sonderrechte", so wie im Übrigen der Notruf auch im Mobilfunknetz „Vorrang" genießt. Dass die computerassistierte

---

[43] Da im Bereich der Telekommunikation die staatliche Eigenerbringung verfassungsrechtlich ausgeschlossen ist; s. dazu *Möstl*, in: Maunz/Dürig, Grundgesetz-Kommentar, Loseblatt-Sammlg. (Stand: 68. EL 2013), Art. 87f Rn. 74; im Kontext staatlicher Gewährleistungspflichten *Luch/Schulz* (Fn. 42), S. 69 ff.

[44] Zur E-Daseinsvorsorge grundlegend *Luch/Schulz*, MMR 2009, 19 ff.; *dies*., in: Hill/Schliesky (Hrsg.), Herausforderung E-Government, 2009, S. 305 ff.

Telechirugie[45] und die Krisenkommunikation der Katastrophenschutz- und Polizeibehörden bzw. die damit verbundenen Daten bevorzugt werden müssen, ist einleuchtend, für welche weiteren Dienste dies auch gilt, wird wahrscheinlich unterschiedlich beurteilt werden.

Diese Grundannahme, dass IT nur im Kontext anderer kritischer Infrastrukturen diese besondere Bedeutung teilt, ist anerkannt und findet sich explizit auch im Entwurf des IT-Sicherheitsgesetzes. Das Bundesamt für Sicherheit in der Informationstechnik zählt nicht nur bestimmte Sektoren zu den kritischen Infrastrukturen, sondern benennt auch die jeweils zugehörigen kritischen IT-Systeme[46]. Dies bedeutet bspw. für den Bereich „Transport und Verkehr" (also „Luftfahrt, Seeschifffahrt, Bahn, Nahverkehr, Binnenschifffahrt, Straße, Postwesen"), dass „Leitstellen, Prozessleittechnik, Logistikmanagement, Verkehrsmanagement, Verkehrssicherheit und Navigation" als kritische IT-Systeme anzusehen sind. Im Finanz-, Geld- und Versicherungswesen sind dies die „Sicherheit der Kommunikation innerhalb und zwischen den Instituten, branchenspezifische Datenverarbeitungsprogramme, bargeldloser Zahlungsverkehr, Interbankenverkehr und Abrechnungssysteme". Konkretisiert werden soll dies im Kontext des IT-SIG-E auf „diejenigen informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind". Im rechtlichen Sinn ist damit eine „dreifache Relevanzprüfung" angelegt: in einem ersten Schritt ist ein bestimmter Infrastrukturbereich als „kritisch" zu klassifizieren, wobei sich diese Einstufung – in Stufe zwei – lediglich auf die „systemrelevanten" Teile dieser Infrastruktur bezieht. In einem dritten Schritt strahlt diese besondere Bedeutung auf die für den maßgeblichen Teil der Infrastruktur maßgeblichen IT-Systeme aus[47].

Daneben lässt sich aber auch festhalten, dass zumindest Teile des Internets, vor allem der Telekommunikationsinfrastruktur, auf der es basiert, aufgrund der beschriebenen Bedeutung – nicht für andere kritische Infrastrukturen, sondern allgemein für das gesellschaftliche, wirtschaftliche Leben – als kritische Infrastruktur einzustufen sind. Wie bei anderen kritischen Infrastrukturen strahlt dies dann auch auf diejenigen IT-Strukturen aus, die für die Funktionsfähigkeit des Internets erforderlich sind.

---

[45] Die technischen Anforderungen dürften sich seit der ersten transatlantischen Operation im Jahre 2001 noch erhöht haben; vgl. dazu Dtsch Ärztebl 2001, A-2465: „Voraussetzung für den Eingriff [war], dass die France Telecom große Übertragungskapazitäten (zehn Megabit pro Sekunde) mittels Glasfaserkabel bereitgestellt hatte. So konnten die Bilder in nur 130 Millisekunden über den Atlantik geschickt werden, wodurch beinahe simultan operiert werden konnte."

[46] Oben Fn. 9.

[47] *Schulz/Tischer,* ZG 2013, 339 (352).

F. Bedrohungsszenarien, Abhängigkeiten und Auswirkungen

Unter dem Begriff Bedrohung wird im Allgemeinen ein potenzielles Ereignis verstanden, dessen Auftreten zu einem wahrnehmbaren Schaden für bzw. an Personen, Organisationen oder anderen Körperschaften führt. Das Auftreten eines solchen Ereignisses wird als stochastischer Wert kalkuliert. Schaden und Schadenshöhe werden i. d. R. monetär berechnet.

Im Rahmen des dynamischen Risikomanagements werden neben Schadenshöhe und Eintrittswahrscheinlichkeit, auch Bedrohungsszenarien betrachtet. Ein Bedrohungsszenario, d. h. eine logisch zusammenhängende Kette von Ereignissen, beschreibt diese Ereignisse i. d. R. in einem Kontext, d. h. in Beziehung zu einer spezifischen Anwendung, zu einem System oder zu einer Organisation. Zusätzlich zu den bedrohlichen Ereignissen kann ein Bedrohungsszenario um eine Reihe von Kontextinformationen angereichert werden, die u. a. auslösende bzw. initiale Ereignisse identifizieren, system- oder organisationsbezogene Schwachstellen benennen und genauere Angaben zur schwere und Art der Schadwirkung beinhalten.

Bei der Entwicklung und Planung kritischer Systeme und Infrastrukturen werden Bedrohungsszenarien als Teil einer Bedrohungsanalyse identifiziert, analysiert und dokumentiert. Auf Basis einer solchen Bedrohungsanalyse können wirksame Gegenmaßnahmen identifiziert und integriert werden. Gegenmaßnahmen dienen dazu, die Wahrscheinlichkeit des Auftretens der Bedrohung zu minimieren oder die resultierende Schadwirkung zu reduzieren. Bedrohungsanalyse und Gegenmaßnahmen sind die Grundlage für ein umfassendes Risikomanagement, mit dem die identifizierten Systemrisiken kontinuierlich dokumentiert, minimiert und kontrolliert werden können.

I. Technische Bedrohungsszenarien und Auswirkungen

In der Informations- und Kommunikationstechnik werden Bedrohungen behandelt, die im Zusammenhang mit informationsverarbeitenden Systemen auftreten sowie durch die Interaktion mit diesen Systemen entstehen bzw. deren Schadwirkung zumindest transitiv über informationsverarbeitende Systeme propagiert wird. Ereignisse, Schadwirkungen und ihre Folgen bleiben jedoch nicht auf die informationsverarbeitenden Systeme beschränkt, sondern interagieren und wirken abhängig vom Zweck des Systems direkt mit der umgebenen physikalischen Welt. Mit dem Begriff Sicherheit ist die Abwesenheit einer Bedrohung, die geringe Wahrscheinlichkeit ihres Auftretens bzw. die reduzierte Schadwirkung assoziiert.

Bei technischen Systemen wie dem Internet werden i. d. R. zwei verschiedene Arten von Sicherheit betrachtet. Unter dem Begriff *Betriebssicherheit* wird der störungsfreie Betrieb eines Gerätes, Systems oder einer Infrastruktur verstanden. Im

Vordergrund stehen hier Bedrohungsszenarien, die stochastisch auftreten und deren Ursprung entweder im System selber (funktionale Störung) oder in nicht-intentionalen äußeren Ereignissen (z. B. Naturkatastrophen, funktionale Störungen oder Ausfälle benötigter Versorgungs- und Betriebseinheiten) liegt. In Abgrenzung dazu befasst sich der Begriff der *IT-Sicherheit* mit dem Schutz vor intentionalen Ereignissen, sog. Angriffen[48]. Die IT-Sicherheit betrachtet dabei im Besonderen den Schutz technischer Systeme vor Angriffen, die die Vertraulichkeit[49] der in den Systemen verarbeiteten Informationen gefährden, die Verfügbarkeit[50] der Systeme und ihrer Dienste unterminieren oder die Integrität[51] der erbrachten Dienstleistungen bedrohen.

Im Sinne der Begriffe Betriebssicherheit und IT-Sicherheit lassen sich Bedrohungsszenarien im Internet entweder als störungsbedingte (nicht-intentionale) Ausfälle oder intentionale Angriffe klassifizieren. Maßgebend für die Klassifizierung ist der Auslöser, d. h. die Ursache der Bedrohung. Schaden und Schadwirkung können sich unabhängig vom Auslöser durchaus ähneln oder gleichen.

Darüber hinaus ist zu unterscheiden, ob die Sicherheit des Internets an sich, d. h. des Internets als eigenständige Infrastruktur, betrachtet wird oder ob die Sicherheit von Infrastrukturen und Anwendungen betrachtet werden soll, die auf dem Internet als Basisinfrastruktur beruhen. Beide Perspektiven haben eine Reihe von Gemeinsamkeiten, erfordern aber durchaus eine andere Gewichtung bei der Betrachtung und Bewertung der Bedrohungsszenarien. Grundsätzlich ist das Internet keine Sicherheitsinfrastruktur. Angriffe auf die Verfügbarkeit, Integrität und Vertraulichkeit des Datenverkehrs sind generell möglich und müssen bei internetbasierten Lösungen selbst dann, wenn zusätzliche Absicherungsmaßnahmen getroffen werden, in Betracht gezogen werden. Internetbasierte Anwendungen und Infrastrukturen sind grundsätzlich weltweit erreichbar und bieten allein schon deshalb eine Angriffsfläche, die es bei nicht-vernetzten bzw. separat vernetzten Lösungen nicht gibt. In den folgenden Abschnittes werden solche Bedrohungsszenarien nur am

---

48 Für einige Fachleute ist die Betriebssicherheit in der Verfügbarkeit und Integrität, wie sie im Rahmen der IT-Sicherheit diskutiert wird, enthalten. Vorzugswürdig erscheint demgegenüber, die Ursachen der Bedrohungen (intentional, nicht intentional) differenzieren zu können, da diese insbesondere bei Einschätzung der Eintrittswahrscheinlichkeit von Belang sind.

49 Vertraulichkeit beschreibt die Wahrung von Geheimnissen und in diesem Sinne den Schutz vor Informationsweitergabe an unbefugte Personen, Organisationen oder Systeme. Vertraulichkeit ist notwendige Grundlage zur Aufrechterhaltung der Privatsphäre sowie zur Wahrung von Staats- und Geschäftsgeheimnissen.

50 Der Begriff Verfügbarkeit beschreibt die Eigenschaft eines technischen Systems, seinen eigentlichen Zweck operativ zur Verfügung zu stellen.

51 Der Begriff Integrität steht für die Gewährleistung der Konsistenz und Genauigkeit von Daten über den gesamten Datenlebenszyklus. In diesem Sinne ist sicherzustellen, dass Daten nicht unautorisiert bzw. unentdeckt modifiziert werden können.

Rande betrachtet. Der Schwerpunkt liegt auf der Betrachtung von Bedrohungsszenarien, die das Internet als Infrastruktur an sich betreffen und die ernsthafte Einschränkungen bzgl. Verfügbarkeit, Integrität und Vertraulichkeit des Internets bzw. seiner grundlegenden Dienste zur Folge haben.

1. Störungen und Angriffe entlang der materiell-geographischen Struktur des Internets

Obwohl das Internet logisch eine dezentrale Struktur aufweist, gibt es zentrale Knoten, die für die Verfügbarkeit der Internetdienste eine zentrale Stellung einnehmen. Hierzu gehören die großen Internetbackbones und die zentralen Übergänge zwischen diesen Backbones. Im europäischen Raum hat sich hierfür der Begriff Internet Exchange Point (IXP) etabliert. Weltweit existieren ca. 300 IXP[52], von denen sich ca. 160 in Europa und ca. 80 in Nordamerika befinden. Der weltweit größte IXP ist der German Commercial Internet Exchange (DE-CIX) in Frankfurt am Main. Die technische Infrastruktur des DE-CIX ist auf verschiedene Rechenzentren über das Frankfurter Stadtgebiet verteilt und weist eine teils redundante, sternförmige Topologie auf. Große IXP wie der DE-CIX in Frankfurt am Main oder der AMS-IX in Amsterdam wickeln nach eigenen Angaben einen großen Teil des Internetverkehrs ab und haben den Datendurchsatz in der Größenordnung eines der großen Internet Service Provider (z. B. die Deutsche Telekom oder AT&T)[53]. Das tatsächlich über einen IXP realisierte Kommunikationsaufkommen ist von außen nicht messbar. Eine Studie zeigt jedoch, dass die tatsächliche Bedeutung der großen IXP für die Kommunikation und Konnektivität im Internet noch weitaus größer ist als bisher angenommen[54]. Störungen, Teil- oder Totalausfälle einer solchen Infrastruktur hätten massive Auswirkungen auf den nationalen und internationalen Internetverkehr. Sie können grundsätzlich durch interne Konfigurationsfehler verursacht werden oder durch äußere Bedrohungen, insbesondere materieller Natur, ausgelöst werden. Angriffe über das Internet sind prinzipiell denkbar, erfordern aber einen hohen Aufwand und einen bisher nicht bekannten Zugriff auf die in einem CIX verwendete Software und Hardware.

Aufgrund der Redundanz und Verteilung der Knoten ist ein Totalausfall eines IXP eher unwahrscheinlich, aber nicht auszuschließen, insbesondere dann, wenn Terrorismus und Krisensituationen betrachtet werden. Obwohl es bisher wohl noch keinen Fall von materieller Zerstörung eines IXP gegeben hat, sind Fälle bekannt, die

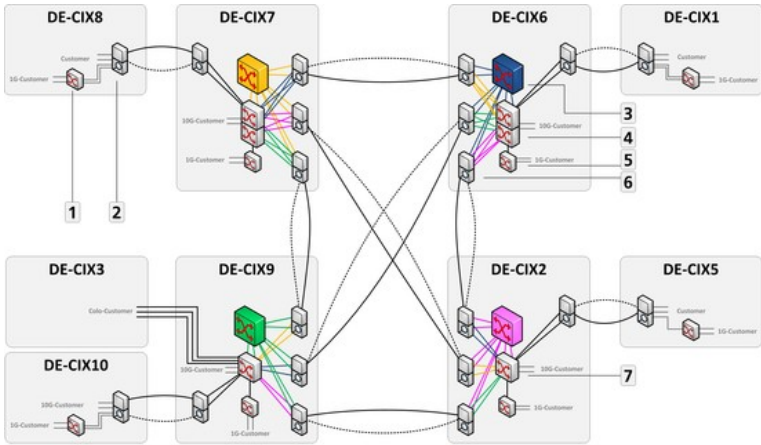
---

52 Euro-IX—European Internet Exchange Association. https://www.euro-ix.net/resources.

53 http://de.wikipedia.org/wiki/German_Commercial_Internet_Exchange.

54 *Ager u. a.,* in: Eggert u. a. (Hrsg.), Proceedings of the ACM SIGCOMM 2012 conference on Applications, technologies, architectures, and protocols for computer communication, 2012, S. 163 ff.

als Störungen durch andere interne und externe Ursachen klassifiziert werden konnten[55]. Die **Fehler! Verweisquelle konnte nicht gefunden werden.**zeigt die verteilte Struktur des DE-CIX Netzes in Frankfurt am Main.



1 Alcatel-Lucent 7210 SAS-M
2 ADVA FSP3000R7 for Remote-Locations
3 Alcatel-Lucent 7950XRS20 Core-Node
4 Alcatel-Lucent 7950XRS40 Edge-Node
5 Alcatel-Lucent 7210 SAS-M
6 ADVA FSP3000R7 for Interconnect-Connections
7 Alcatel-Lucent 7950XRS20 Edge-Node

ABBILDUNG 2: TOPOLOGIE DES DE-CIX (QUELLE: DE-CIX)

Der interkontinentale Internetverkehr wird maßgeblich über am Meeresgrund verlegte Glasfaserkabel realisiert. Die Kabel selbst sowie die Übergangspunkte an Land sind zentrale Grundlage für den Internetverkehr. Durch die komplexe geographische Verteilung von Internetdiensten sowie die komplexen Peering-Beziehungen der ISP können Störungen an den großen Interkontinentalverbindungen zusätzlich zu dem eigentlichen Verbindungsverlust auch Auswirkungen auf den gesamten Internetverkehr haben. Im März 2013 kam es bspw. in Ägypten und Indien zu erheblichen Internetausfällen, weil das SMW4-Seekabel — ein Glasfaserkabel mit einer Kapazität von 1.280 Gbit/s vor der Nordküste Ägyptens — an mehreren Stellen durchtrennt wurde. Laut Presseinformationen fielen dabei 70 % der ägyptischen Netzkapazität und die Hälfte der indischen Kommunikationsbandbreite aus[56].

[55] http://de.wikipedia.org/wiki/German_Commercial_Internet_Exchange.

[56] In Indien waren hauptsächlich private Anwender betroffen. Die großen, professionellen Kunden (Kommunikationsdienstleister, IT-Firmen, Call-Center) konnten durch die Nutzung in Indi-

Bis heute ist unklar, ob es sich dabei um Sabotage oder, wie der Betreiber mitteilte, um Zerstörungen durch Schiffsschrauben handelte. Die nachfolgende **Fehler! Verweisquelle konnte nicht gefunden werden.**zeigt eine Übersicht über die Seekabelverbindungen und die entsprechenden Übergabepunkte an Land.

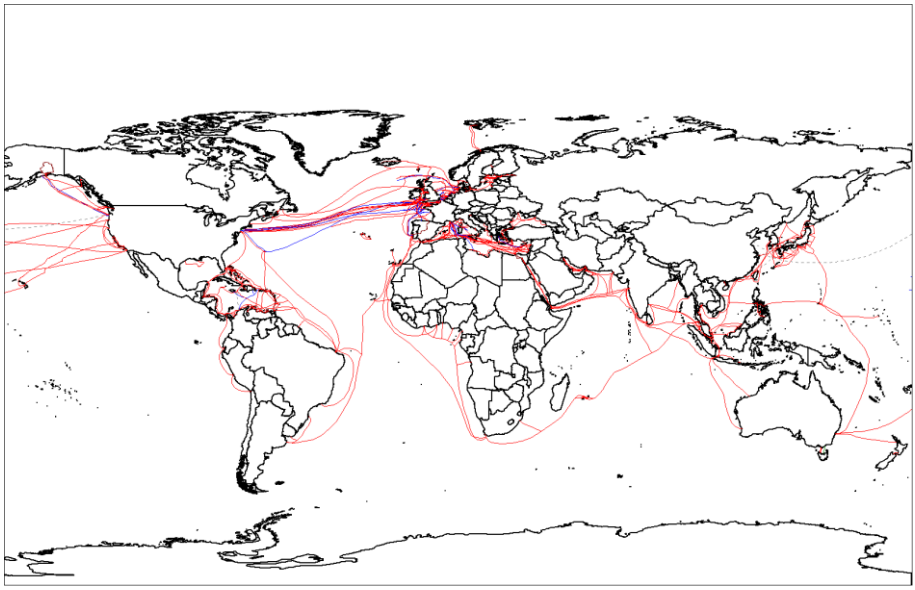


ABBILDUNG 3: VERLAUF DER UNTERSEEKABEL (QUELLE: WIKIPEDIA)

Interessant ist hier, dass insbesondere die Übergabepunkte zentrale Stellen sind, an denen jeweils mehrere Seekabel an einer Stelle zusammengeführt und damit Knoten geschaffen werden, die Angriffen unterschiedlichster Natur ein zentrales Ziel bieten. Ein Beispiel hierfür sind die unlängst publik gemachten Aktivitäten des britischen Geheimdienstes[57], der sich umfassenden Zugriff auf die transatlantisch kommunizierten Internet- und Telefondaten, u. a. auch aus Deutschland, verschafft hat.

---

en vorhandener, redundanter Leitungen die Auswirkungen in ihren Geschäftsbereichen minimieren.

[57] Im Rahmen der Operation „Tempora“ hat sich der Government Communications Headquarters (GCHQ) systematisch Zugang zu Internet- und Telefondaten u. a. auch aus Deutschland verschafft. Der Zugriff auf die Daten erfolgte über das Glasfaserkabel TAT-14, über das ein großer Teil der deutschen Übersee-Kommunikation abgewickelt wird (s. auch http://www.heise.de/newsticker/meldung/Bericht-GCHQ-schoepft-deutsches-Internet-am-Ueberseekabel-ab-1895776.html).

Die materiell-geographische Struktur des Internets ist zentralisierter als sich vermuten lässt. Es gibt physikalische Knoten an denen der Internetverkehr zentral gestört, manipuliert und abgehört werden kann. Störungen und Angriffe an den zentralen physikalischen Infrastruktureinheiten des Internets können massive Einschränkungen bezüglich der Verfügbarkeit von Internetdiensten zur Folge haben und bieten die Möglichkeit, Verfügbarkeit, Vertraulichkeit und Integrität der über das Internet kommunizierten Informationen in größerem Stil zu beeinträchtigen.

2. Störungen und Angriffe entlang der softwarebasierten Struktur des Internets

Neben den zentralen physikalischen Trägern der Internetkommunikation, d. h. den physikalischen Kommunikationsverbindungen sowie den Übergabepunkten, gibt es zentrale softwarebasierte Dienste und Protokolle, die maßgeblich für das Funktionieren des Internets sind. Als zentral sind insbesondere zu erachten:

- die paketvermittelte Kommunikation, Nutzkanal-Signalisierung (in-band signalling) sowie ihre Beschränkungen bezüglich Datendurchsatz und Latenz,
- das Routing, d. h. die Entscheidung darüber, welchen Weg die Informationspakete einer paketvermitteltеten Kommunikation durch das Internet nehmen,
- die Namensauflösung in Form des Domain Name Systems sowie
- die Sicherheits- und Zertifikatsinfrastruktur zur Absicherung der Internetprotokolle, d. h. die kryptographischen Verfahren, die zur Absicherung der Internetkommunikation verwendet werden, und die Anbieter von Sicherheitslöungen sowie ihre Soft- und Hardwareinfrastruktur, die als Grundlage für eine Authentisierung im Internet verwendet wird.

Störungen und gezielte Angriffe auf einen dieser Bereiche können ebenso wie ein Angriff oder eine Störung der materiellen Infrastruktur massive Einschränkungen bezüglich der Verfügbarkeit von Internetdiensten zur Folge haben und bieten die Möglichkeit, Verfügbarkeit, Vertraulichkeit und Integrität der über das Internet kommunizierten Informationen in größerem Stil zu beeinträchtigen. Im Unterschied zu Angriffen auf die materielle Struktur setzt ein Angriff auf die softwarebasierte Infrastruktur nicht unbedingt einen physischen Zugang zur Infrastruktur voraus und kann prinzipiell weltweit erfolgen.

3. Störungen und Angriffe auf die paketvermittelte Kommunikation

Die Internetkommunikation basiert auf paketvermittelter, zunächst verbindungsloser Kommunikation und der gemeinsamen Übertragung von Nutzerdaten und

Kontrollinformationen über einen Kommunikationskanal. Aus diesem Grund ist die Erzeugung und Einbringung von IP-Paketen zu Angriffszwecken ohne Schwierigkeiten möglich, wenn ein Rechner bereits mit einem Netzwerk verbunden ist.

Denial-of-Service-Angriffe (DoS) oder ihre verteilte Form, die Distributed-Denial-of-Service-Angriffe (DDoS), sind ein Versuch, die Verfügbarkeit eines Systems oder eines Netzwerks einzuschränken bzw. komplett zu stören. Solche Angriffe bestehen in der Monopolisierung prinzipiell endlicher Ressourcen eines bestimmten Systems oder Netzwerks. Sie beruhen i. d. R. darauf, dass über einen längeren Zeitraum hinweg viele Kommunikationsverbindungen von vielen Orten gleichzeitig zu einer Internetressource aufgebaut werden, sodass diese Ressource ihr Leistungsmaximum erreicht und nicht mehr für die ursprüngliche Aufgabe zur Verfügung steht. Ausfallzeiten von Stunden oder sogar Tagen können die Folge sein.

Im Jahr 2007 war Estland über drei Wochen lang einer Serie politisch motivierter Cyber-Angriffe ausgesetzt. Diese Angriffe reichten von der einfachen Manipulation von Webseiten (Defacement) über länger anhaltende DDoS-Angriffe auf an das Internet angeschlossene Infrastrukturen wie Banken bis hin zu Einschränkungen der Verfügbarkeit von Internet Service Providern[58]. Letzteres lässt sich durchaus als ein Angriff auf die Basisinfrastruktur des Internets begreifen.

4. Angriffe auf die Routinginfrastruktur

Routingprotokolle dienen zum Austausch von Routing- und Netzinformationen und werden zum Aufbau der Routing-Tabellen in den Gateways der Netzwerkbetreiber verwendet.

Besondere Bedeutung hat derzeit das Border Gateway Protocol (BGP). Es ist das einzige Protokoll, das als Routing-Protokoll zwischen den großen autonomen Systemen (AS) des Internets verwendet wird. Unter einem AS versteht man im Kontext des Internets eine Zusammenstellung von verbundenen Internet Protocol-Adressen (IP-Adressen), die unter der Kontrolle von einem oder mehreren Netzbetreibern stehen und für die es eine gemeinsame, klar definierte Routing-Policy gibt. Störungen, Ausfälle und Manipulationen in diesem Bereich haben große Auswirkungen auf die Erreichbarkeit einzelner Netze sowie für den globalen Internetverkehr. Manipulationen in diesem Bereich führen in letzter Konsequenz zu einer Neustrukturierung des Internetverkehrs. Da die Mechanismen des Routings nicht unter der Kontrolle des Anwenders liegen, muss dieser der Infrastruktur vertrauen. Im Folgenden sind die wichtigsten Angriffe auf ein BGP-basiertes Routing beschrieben:

---

[58] Vgl. *Czosseck/Ottis/Talihärm,* in: Ottis (Hrsg.), Proceedings of the 10th European Conference on Information Warfare and Security, 2011, S. 57 (57).

- Manipulation der Routen, sodass der Internetverkehr über ein vom Angreifer kontrolliertes Gateway geleitet wird (Redirection, Spoofing). Dies kann entweder mit dem Ziel passieren, den betroffenen Internetverkehr gezielt abzuhören, zu manipulieren (Traffic Subversion) oder zu unterbinden (Blackholing).
- Vollständiges Entfernen von Routen, sodass in bzw. mit einem bestimmten Adressbereich kein Internetverkehr mehr möglich ist.
- Destabilisierung des Netzwerks, indem die gewollten Verzögerungen beim Ändern der Routen, das sog. Route Flap Damping (RDF), dazu verwendet werden, durch sukzessive Routenänderungen die Konnektivität des Netzes zu stören[59]. Ein einzelner BGP-Lösch- und Annoncierungszyklus kann ein angeschlossenes Netzwerk für einen Zeitraum von bis zu einer Stunde nicht erreichbar machen[60]. Wird ein solcher Vorgang absichtlich immer wieder in Gang gesetzt, kann ein Netzwerksegment längerfristig aus dem Verkehr gezogen werden.

BGP-basierte Eingriffe in das Internet sind durchaus bekannt. So blockiert bspw. China den Zugang zu google.com seit 2002 über diesen Mechanismus[61]. Weiterhin beruht einer der größten weltweiten Ausfälle der Youtube.com-Plattform auf einer BGP-Fehlkonfiguration im pakistanischen Internet, der die Plattform aus dem gesamten Internet für zwei Stunden unerreichbar machte[62]. Im November 2013 berichtet die Firma Renesys über eine Reihe von Vorfällen, die die Interpretation zulassen, dass Routen im Internet gezielt und temporär manipuliert werden. Renesys beobachtete, dass Teile des Internetverkehrs auf Routen zum Ziel geleitet werden, die nach technischen und ökonomischen Kriterien nicht sinnvoll sind[63].

Routing basiert ursprünglich auf einem kooperativen Modell, bei dem davon ausgegangen wurde, dass auch zwischen Routern unter verschiedener administrativer Hoheit nur vertrauenswürdige Informationen ausgetauscht werden. Über die Re-

---

59 *Sriram u. a.,* IEEE Journal on Selected Areas in Communications 24 (2006), S. 1901 ff.

60 *Mao u. a.,* in: SIGCOMM '02 – Proceedings of the 2002 conference on Applications, technologies, architectures, and protocols for computer communications, 2002, S. 221 ff.

61 BBC NEWS: china blocking google, http://news.bbc.co.uk/1/hi/technology/2231101.stm.

62 YouTube hijacking: A RIPE NCC RIS case study RIPE network coordination centre, http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study.

63 Im Juli und August 2013 registrierte Renesys mehrere Umleitungen des Internetverkehrs zwischen zwei Internet-Providern in Denver, Colorado über Island. Zuvor war bereits mehrmals aufgefallen, dass Daten für amerikanische Internet-Provider über mehrere Monate hinweg scheinbar unsinnigerweise über Weißrussland geroutet wurden (http://www.renesys.com/2013/11/mitm-internet-hijacking/).

source Public Key Infrastructure (RPKI)[64] lassen sich Routing-Informationen über Zertifikate absichern, sodass nur valide Informationen von Routern ausgewertet werden.

5. Störungen und Angriffe auf das Domain Name System DNS

Das Domain Name System ist ein verteiltes System mit der Aufgabe, die menschenlesbare Domain-Namen und die korrespondierenden maschinenlesbaren IP-Adressen einander zuzuordnen und diese Zuordnung über das Internet zu propagieren. Das DNS ist hierarchisch organisiert. Jede Domain ist durch die Nennung eines autorisierten Nameservers gekennzeichnet. Ein solcher autorisierter Nameserver ist für die Auflösung von Namen und Adressen der jeweiligen Domain zuständig. Er kann seine Aufgabe delegieren, d. h., seine Funktionalität durch einen autorisierten Nameserver einer Unterdomäne realisieren lassen. An der Spitze dieser Hierarchie stehen 13 sog. Root-Server. Diese Server sind die zentralen DNS-Server im Internet und auf globaler Ebene die Verknüpfung zwischen den Domain-Namen und den numerischen Rechneradressen.

Das DNS basiert darüber hinaus auf dem sog. DNS-Protokoll, d. h. einer detaillierten Beschreibung der Datenstrukturen und Kommunikationsabläufe, die eine Hierarchie der DNS-Server grundsätzlich realisiert und den notwendigen Informationsaustausch zwischen den Servern ermöglicht.

Das DNS bzw. das entsprechende Protokoll wurde ursprünglich nicht als sicheres Protokoll entwickelt, eine grundlegende Unterstützung für die Datenintegrität, Authentifizierung und Autorisierung fehlt. Um das DNS im Hinblick auf seine IT-Sicherheitseigenschaften robuster zu machen, wurden Ende 1997 durch die Internet Engineering Task Force (IETF) die Domain Name System Security Extensions (DNSSEC) als Erweiterung des bisherigen Standards vorgeschlagen, welche durch den Einsatz kryptographischer Verfahren Datenintegrität und Authentifizierung bereitstellt. DNSSEC stellt erhebliche organisatorische Anforderungen an die Schlüsselverwaltung sowie die Signiervorgänge. Zudem musste das neue Protokoll derart eingeführt werden, dass bestehende Netzwerkkomponenten durch das neue Protokollelement nicht in ihrer Funktionsweise beeinträchtigt werden. Für die Top Level Domain „.de“ ist DNSSEC seit Mai 2011 aktiv und wird als optionales Sicherheitsfeature angeboten[65].

---

[64] S. auch http://www.heise.de/netze/meldung/RPKI-Angst-vor-einem-Staatshack-1930050.html

[65] http://www.denic.de/domains/dnssec.html.

In der Literatur finden sich eine Reihe von Bedrohungsszenarien, die sich direkt auf das DNS beziehen:

- Angriffe auf die Verfügbarkeit des DNS, sodass der Service nur noch teilweise oder gar nicht mehr zur Verfügung steht
  - Gezielte DDoS-Angriffe können DNS-Server mit zum Zwecke des Angriffs erzeugten Anfragen so unter Last setzen, dass sie ihren eigentlichen Service nicht mehr anbieten können.
- Angriffe auf die Integrität der Serverdaten mit dem Ziel, falsche DNS-Auskünfte zu erteilen. Hierdurch können Host-Namen-basierte Anfragen umgeleitet bzw. in Leere laufen gelassen werden. Die folgenden Angriffsmöglichkeiten sind bekannt:
  - Übernahme bzw. Fälschung von Nachrichten, die mit Hilfe des DNS-Protokolls übertragen werden (DNS Spoofing).
  - Fälschung von Daten, die in den Datenbanken und Zwischenspeichern der einzelnen DNS-Server liegen (Cache Poisoning)
- Angriffe auf die Vertraulichkeit der DNS-Anfragen, um Kommunikationsprofile erstellen zu können. Auch das DNS-Protokoll eignet sich dazu, Metadaten der Kommunikation, d. h.: wer kommuniziert zu welchem Zeitpunkt mit welchem Server, systematisch zu sammeln und zu dokumentieren.

Darüber hinaus kann auch eine einfache Fehlkonfiguration eines DNS Servers dazu führen, dass größere Teile des DNS in Mitleidenschaft gezogen werden.

Beispiele für Angriffe auf das DNS gibt es einige. So wurde im Oktober 2002 ein massiver DDoS-Angriff auf die Root-Server des Internets registriert. Insgesamt waren neun der 13 Root-Server ca. eine Stunde lang einem ICMP-Flooding genannten DDoS-Angriff ausgesetzt[66]. Am 6. 2. 2007 wurde ein weiterer Angriff registriert, der sich insgesamt über 24 Stunden hinzog und die Verfügbarkeit von mindestens zwei der 13 Root-Server stark beeinträchtigte[67]. Im August 2013 war China Ziel eines

[66] Am 21. 10. 2002 wurde auf die 13 Root Server des Internets etwa eine Stunde lang ein DDoS-Angriff ausgeführt. Angeblich sei dies der größte und komplexeste DDoS-Angriff gewesen, der bis dahin gegen das Root-Server-System gerichtet wurde. Insgesamt war dies der zweite wichtige Ausfall der DNS-Root-Server. Der erste Ausfall wurde aufgrund technischer Probleme im April 1997 verursacht.

[67] ICAN Factsheet: Root Server Attack on 6 February 2007, http://www.icann.org/en/about/learning/factsheets/factsheet-dns-attack-08mar07-en.pdf.

solchen Angriffs, bei dem über zwei Stunden lang Teile des chinesischen Internets lahmgelegt oder gestört wurden[68].

Während erfolgreiche DDoS-Angriffe gegen die 13 Root-Server inzwischen als eine rein theoretische Bedrohung[69] betrachtet werden können, bleibt die Verletzbarkeit im Zugangsnetzwerk gegeben.

6. Störungen und Angriffe auf die Sicherheits- und Zertifikatsinfrastruktur

Die Sicherheit der Internetprotokolle und ihre sichere Verwendung für die grundlegenden Kommunikationsaufgaben im Internet hängt von der Sicherheit kryptographischer Verfahren, der verwendeten Sicherheitssoft- und -hardware sowie der sicheren Verwahrung von Zertifikaten und der dazugehörigen Schlüssel ab. Kryptographische Verfahren und deren Realisierung in Soft- und Hardware bilden u. a. die Grundlage für Sicherheitserweiterungen des DNS (DNSSEC) wie auch für das Routing. Aktuelle Angriffe u. a. aus dem Umfeld von Geheimdiensten haben gezeigt, dass auch eine solche bisher als sicher eingestufte Infrastruktur als nicht sicher angenommen werden muss. Beispiele aus der jüngeren Vergangenheit sind der Angriff auf die Zertifikatsinfrastruktur bei DigiNotar[70], die Verwendung gefälschter Zertifikate zur Verkörperung vertrauenswürdiger Kommunikationspartner[71] und die mögliche Einflussnahme der NSA auf die Standardisierung kryptographischer Verfahren wie bspw. der NIST-Reihe 800-90[72].

---

68 http://www.handelsblatt.com/politik/international/cyberattacke-china-groesster-angriff-auf-sein-internet-/8700660.html.

69 Die Root-Nameserver-Infrastruktur ist in den letzten Jahren durch eine Kombination von Anycast- und Lastausgleichstechniken erweitert worden. Die meisten der 13 Root-Server wurden als global verteiltes Server-Cluster in mehreren Rechenzentren realisiert. Dadurch ist eine Serverinfrastruktur entstanden, die hoch belastbar und verteilt arbeitend ihre Verwundbarkeit speziell gegen DDoS-Angriffe, wie sie in den Jahren 2002 und 2007 stattgefunden haben, verloren hat.

70 Am 19. 7. 2013 hat das niederländische Unternehmen DigiNotar einen Angriff auf seine Zertifikatsinfrastruktur entdeckt. Die unbekannten Angreifer waren in die Server des Sicherheitsdienstleisters eingedrungen und hatten dort sog. SSL-Zertifikate erstellt, mit denen sie sich unter anderem als Google ausgeben konnten.

71 Inzwischen ist bekannt geworden, dass sowohl der französische Geheimdienst wie auch die NSA gefälschte bzw. fälschlicherweise ausgestellte Zertifikate nutzen, um durch Man-in-the Middle-Angriffe Zugriff auf vertrauliche Kommunikationsdaten zu erhalten (s. https://www.schneier.com/blog/archives/2013/09/new_nsa_leak_sh.html).

72 Die Publikationen der NIST Reihe 800-90 betreffen Pseudo-Zufallszahlengeneratoren, die als Grundlage fast aller kryptographischen Verfahren unabdingbar sind. Der von NIST 2007 als Dual_EC_DRBG-Standard vorgeschlagene Zufallsalgorithmus enthält eine Schwachstelle, die nach einem Artikel der New York Times (http://www.nytimes.com/2013/09/06/us/nsa-foils-

7. Zusammenfassung

Jüngere Ereignisse wie auch die kurze Geschichte des Internets bieten einen Vorgeschmack bzw. eine Vorahnung, welche Dimensionen insbesondere gezielte Störungen, Manipulationen und Vertraulichkeitsverletzungen von Daten im Internet haben können. Das daraus resultierende Bedrohungsspektrum ist vielfältig und reicht vom einfachen Aufzeichnen der Daten und Metadaten zum Zwecke des Ausspähens von Geschäfts- und Staatsgeheimnissen oder zum Zwecke der (staatlichen) Überwachung von Kommunikationsbeziehungen über die Manipulation von Daten und Routen mit dem Ziel, Zugriff auf fremde Ressourcen zu bekommen oder den Zugriff auf Ressourcen im großen Stil zu verhindern, bis hin zur Zerstörung der für den Betrieb einer Infrastruktur notwendigen Hard- und Software, wie es bspw. im Fall Stuxnet als Teil einer Cyber-War-Strategie betrieben wurde.

Die Ursachen, Täter und ihre Motive, die hinter den einzelnen Bedrohungsszenarien liegen, sind so vielfältig wie die Bedrohungsszenarien selber. Sie reichen von einfachen Bedien- und Konfigurationsfehlern über Hacker, die sich aus Neugier oder falsch verstandenem Ehrgeiz am Internet ausprobieren, Korruption, organisierte Kriminalität, Wirtschaftsspionage, Terrorismus bis hin zu Geheimdiensttätigkeiten und Cyber-War, bei dem sich feindlich gesonnene Staaten durch gezielte Angriffe zu schädigen versuchen.

Grundsätzlich muss mit Bedrohungen gerechnet werden, die sowohl das Internet als Infrastruktur beeinträchtigen wie auch an das Internet angeschlossene Systeme und Infrastrukturen schädigen bzw. in ihrer Funktionalität beeinträchtigen können. Bedrohungsszenarien, die an das Internet angeschlossene Systeme und Infrastrukturen schädigen bzw. in ihrer Funktionalität beeinträchtigen, sind in der Realität weitaus häufiger und vielfältiger als die oben beschriebenen Bedrohungsszenarien für das Internet an sich. Sie fokussieren auf das Internet als Übertragungsmedium und profitieren von der weltweiten Erreichbarkeit an das Internet angeschlossener Systeme. Zu diesen Bedrohungsszenarien zählen neben der Anfälligkeit für DDoS-Angriffe insbesondere die Infektion und Infiltration von Systemen durch Viren, Würmer und Trojaner, die über das Internet eine bisher noch nicht gekannte Verbreitung gefunden haben.

Bedrohungsszenarien für das Internet an sich sind hingegen deutlich seltener, erfordern, im Falle einer intentionalen Bedrohung (d. h. eines Angriffs), i. d. R. einen höheren logistischen Aufwand bei der Planung und Durchführung, sind aber umso gravierender, was die zu erwartenden Schäden angeht. Durch den Umstand, dass das Internet eine globale und allgemeine Kommunikationsplattform ist, d. h. eine Kommunikationsinfrastruktur für andere Infrastrukturen darstellt, sind die Konse-

---

much-internet-encryption.html?pagewanted=all&_r=0) als Einflussnahme der NSA identifiziert werden kann.

quenzen solcher Bedrohungsszenarien weitaus größer, da in der Regel alle auf dem Internet basierenden Infrastrukturen von einer solchen Bedrohung betroffen sind. Gerade aus dem Verhältnis zwischen Kommunikationsinfrastruktur und Infrastruktur und den diesem Verhältnis zugrunde liegenden vielfältigen Abhängigkeitsbeziehungen entsteht ein Bedrohungspotenzial, das sich häufig nur schwer abbilden und analysieren lässt. Zu betrachten wären hier insbesondere Kaskadeneffekte, die sich aus wechselseitigen Abhängigkeitsbeziehungen, wie sie sich bspw. zwischen Stromversorgung und Kommunikationsinfrastruktur ergeben, die für ihr Funktionieren inzwischen beide aufeinander angewiesen sind.

Wenig beruhigend ist, dass empfindliche Eingriffe in die Internetinfrastruktur vermeintlich einen so hohen logistischen Aufwand erfordern, dass nur größere Akteure einen solchen Angriff wirklich effektiv durchführen können. Die Vergangenheit hat gezeigt, dass das Internet Möglichkeiten zur Potenzierung bietet, die durchaus auch von kleineren Akteuren genutzt werden können, um bspw. effektive DDoS-Angriffe[73] auf zentrale Strukturen des Internets durchzuführen. Zugleich müssen auch staatliche Eingriffe in das Internet kritisch betrachtet werden. Die Eingriffe in das Internet zum Zwecke der Zensur (Beispiel: China) bzw. zum Entzug der internetbasierten Kommunikationssysteme im staatlichen Krisenfall (Beispiele: Ägypten, Syrien) zeigen grundsätzlich, welches kritische Potenzial in der Kontrolle der internetbasierten Kommunikation liegt. Das durch *Edward Snowden* bekannt gewordene Ausmaß an Kontrolle, Manipulation und Vertraulichkeitsverletzungen durch geheimdienstliche Tätigkeiten zeigt, dass auch demokratische Staaten in intransparenter Weise in die Internetkommunikation eingreifen.

Schlussfolgerung: Das Internet muss grundsätzlich als eine „unsichere" Infrastruktur verstanden werden, die an sich durch redundante Strukturen zwar grundsätzlich stabil ist, aber nur unzureichend gegen intentionale Störungen und Manipulationsversuche geschützt ist. Die sichere Nutzung der Infrastruktur Internet ist ohne zusätzliche Absicherung im Zugangsnetz bzw. auf der Ebene der Infrastruktur nicht möglich. Wird die Nutzung des Internet als Kommunikationsinfrastruktur (und damit als essenzielle Basis) für andere kritische Infrastrukturen in Betracht gezogen, sollten die bis hierhin erläuterten Bedrohungsszenarien in ihrer Bedeutung und Konsequenz für die jeweilige Infrastruktur ausführlich betrachtet werden.

[73] Inzwischen stehen auf einer Art Schwarzmarkt sog. Bot-Netze als regelrechte Mietobjekte zur Verfügung. Diese Bot-Netze lassen sich temporär für konzertierte Aktionen im Internet anmieten und nutzen. Durch die mit der Anmietung einhergehende Kontrolle einer größeren Zahl infiltrierter Rechner lassen sich so auch für Einzelakteure größere koordinierte Aktionen (wie bspw. DDoS-Angriffe) im Internet durchzuführen.

II. Exemplarische Betrachtung von Abhängigkeiten

Im Folgenden werden exemplarisch für die Bereiche öffentliche Verwaltung, Gesundheit, Energie und öffentliche Sicherheit Abhängigkeiten skizziert, die potenzielle Bedrohungen heute und für die Zukunft darstellen können. Diese Untersuchungen zeigen, dass – auch wenn derzeit noch kaum großskalig direkt kritische Abhängigkeiten bestehen – diese tendenziell mit der verstärkten Nutzung des Internets ansteigen und sich in Zukunft zu größeren Bedrohungsszenarien entwickeln können. Schon heute bestehende indirekte Auswirkungen, die durch die Verkettung von verschiedenen Ausfällen sowie Angriffsszenarien bei Dritten auch auf „internetfreie" Prozesse Einfluss nehmen können, konnten in dieser ersten Betrachtung dabei noch gar nicht erfasst werden. Grundsätzlich ist analog zu den Erkenntnissen von indirekten Abhängigkeiten bei Stromausfallszenarien[74] durch die Komplexität der heutigen Prozesse und die Verteilung von Aufgaben auf unterschiedlichste Dienstleister mit derartigen indirekten Effekten zu rechnen, die nur äußerst schwer ex-ante identifizierbar sind. Es ist davon auszugehen, dass das Bedrohungspotenzial dieser indirekten Effekte mit der stärkeren Nutzung des Internets tendenziell ansteigt.

1. Öffentliche Verwaltung

Die öffentliche Verwaltung umfasst verschiedene Ebenen von den Kommunen über die Länder bis zum Bund und der EU-Verwaltung. Dabei sind die Abhängigkeit vom Internet (bzw. von eigenen Intranetstrukturen) und öffentlichen IT-Dienstleistern sowie die Vernetzung zwischen verschiedenen Verwaltungen in den höheren Ebenen deutlich stärker ausgeprägt als in der Mehrzahl der Kommunen[75].

Dass unmittelbar sicherheitsrelevante Bereiche der öffentlichen Verwaltung, wie Polizei, Feuerwehr, Geheimdienste oder Militär, zu den kritischen Infrastrukturen gehören, steht außer Frage. Doch die oben eingeführte Definition von kritischen Infrastrukturen[76] als Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe bis hin zu Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten können, trifft auch auf diverse andere Bestandteile der öffentlichen Verwaltung zu.

---

74 Vgl. Reichenbach u. a. (Hrsg.), Risiken und Herausforderungen für die öffentliche Sicherheit in Deutschland: Szenarien und Leitfragen – Grünbuch des Zukunftsforums Öffentliche Sicherheit, 2. Aufl. 2011, S. 16 ff.

75 Zur Abhängigkeit der öffentlichen Verwaltung vom Internet und IT-Infrastrukturen *Schulz*, in: Hill/Schliesky (Hrsg.), Die Vermessung des virtuellen Raums, 2012, S. 265 (269 ff.).

76 S. oben Gliederungspunkt C. III.

Hier sei als Beispiel das Sozialwesen genannt. Mehr als 25 Millionen Menschen in der Bundesrepublik Deutschland beziehen Leistungen der Deutschen Rentenversicherung[77]. Hinzu kommen mehrere Millionen Bezieher von Arbeitslosengeld, Arbeitslosengeld II u. Ä. Diese Leistungen werden in der Regel am letzten Bankarbeitstag des Monats überwiesen, sodass innerhalb eines begrenzten Zeitfensters enorme Summen transferiert werden, die für einen erheblichen Teil der Bevölkerung einen Teil oder die Gänze ihres Lebensunterhalts darstellen. Hier besteht daher schon eine mittelbare Abhängigkeit von den Infrastrukturen des Internets, da die kritischen Infrastrukturen des Finanz-, Geld- und Versicherungswesens, die der Leistungserstattung zugrunde liegen, selbst in großem Maße auf das Internet angewiesen sind. Ein Ausfall des Internets, gerade während des kritischen Zeitraums um den Monatswechsel, würde daher mit Versorgungsproblemen für einen erheblichen Teil der Bevölkerung einhergehen.

Aber auch eine unmittelbare Abhängigkeit von Internetstrukturen besteht. Die Kommunikation zwischen Verwaltungen erfolgt bereits zum größten Teil via E-Mail. Mit dem im Jahr 2013 in Kraft getretenen Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften[78] wird vor allem die Ersetzung der Schriftform im elektronischen Kontakt erleichtert[79] und ermöglicht, dass die elektronische Kommunikation auch zwischen Bürgern und Verwaltung zukünftig die Regel sein kann. Dabei bleibt die Abwicklung über das Internet jedoch auf absehbare Zeit noch eine Option, neben der die traditionelle Schriftform weiterhin angeboten wird. Es ist deshalb davon auszugehen, dass im Falle eines Ausfalls des Internets traditionelle Kommunikationswege wie Briefe und vor allem Telefonnetze zur Kompensation genutzt werden könnten, sodass die Verwaltungen nicht gänzlich außer Funktion gesetzt würden.

Hier ist jedoch noch auf einen weiteren Aspekt hinzuweisen: Gegenwärtig wird auf unterschiedlichen Ebenen der öffentlichen Verwaltung, von kommunalen bis zu gesamteuropäischen Initiativen, die Verlagerung von Datenspeicherung, Software und Funktionen wie z. B. E-Mail-Kommunikation hin zu Cloud-Lösungen betrieben[80]. Damit erhöht sich die Abhängigkeit von den Betreibern der Server und der

---

77 Bundesministerium für Arbeit und Soziales (Hrsg.), Die Rentenbestände in der gesetzlichen Rentenversicherung in der Bundesrepublik Deutschland. Stand: 1. 7. 2012, 2013, S. 17.

78 Vom 25. 7. 2013, BGBl. I S. 2749; dazu *Habammer/Denkhaus*, MMR 2013, 358 ff.; *Müller-Terpitz/Rauchhaus*, MMR 2013, 10 ff.; *Heckmann/Albrecht*, ZRP 2013, 42 ff.; *Ramsauer/Frische,* NVwZ 2013, 1505 ff.; *Albrecht/Schmidt,* K&R 2013, 529 ff.

79 Zu diesem Aspekt *Schulz*, DÖV 2013, 882 ff.; *Prell*, NVwZ 2013, 1514 ff.

80 Hier sei als Beispiel das EU-Projekt „Cloud for Europe" genannt, an dem Fraunhofer FOKUS maßgeblich beteiligt ist und das u. a. die Etablierung einheitlicher Cloud-Standards für die öffentliche Verwaltung innerhalb der Europäischen Union anstrebt; zu Einsatzoptionen von Cloud Computing für die öffentliche Verwaltung *Schulz*, MMR 2010, 75 ff.; *ders*., VM 2010, 36 ff.

Netzinfrastrukturen. Beim Ausfall der Verbindung wären z. B. Daten zu Personenständen oder zum Straßenbau, die zur Verkehrsplanung oder im Notfall zur Identifikation von Personen benötigt werden, nicht mehr abrufbar, da Cloud-Lösungen gerade genutzt werden, um die kostspielige Unterhaltung eigener Server einzusparen. Zudem geht der Trend hin zu Cloud-Strukturen, die von mehreren Verwaltungen gemeinsam genutzt werden. Somit wären beim Ausfall der Verbindung gleich mehrere Verwaltungen betroffen. Die „kritische" Rolle, die das Internet bereits heute für die öffentliche Verwaltung einnimmt, wird sich also in den nächsten Jahren noch verstärken, was den Schutz dieser Infrastruktur umso wichtiger macht.

2. Energie

Energieversorgungsstrukturen gehören unbestritten zu den kritischen Infrastrukturen. In diesem Kontext zählen insbesondere Leitstellen sowie die gesamte Prozessleit- und Steuertechnik zu den kritischen IT-Systemen. So kann ein in böswilliger Absicht geführter Zugriff auf die Anlagensteuerung eines Kraftwerks verheerende Folgen haben. Dass ein solches Szenario Realität werden kann, zeigt spätestens die Existenz des Computerwurms „Stuxnet" zur Beeinflussung der Leittechnik einer kerntechnischen Anlage[81].

Durch gegenwärtigen Umbau der Stromversorgung von einem zentral gesteuerten, hierarchisch organisierten, relativ statischen und geschlossenen Versorgungssystem hin zu einem offenen, dezentral organisierten, flexiblen System mit vielen Akteuren ergibt sich ein erhöhter Kommunikationsaufwand sowie die Notwendigkeit der Speicherung und Verarbeitung großer Datenvolumen. Das bedeutet, dass entweder bestehende kommunikations- und informationsverarbeitende Infrastrukturen genutzt werden können oder neue geschaffen werden müssen. Ob dabei das Internet und die bestehenden Internetzugänge – wie z. B. bestehende DSL-Anschlüsse – genutzt werden, hängt von jeweiligen Anforderungen und den damit verbundenen Risiken ab. Während die Übertragung von individuellen Energieverbrauchsdaten aus sog. „Smart Metern" zur Erstellung von Abrechnungen hohe Anforderungen an Datenschutz stellt[82], spielt die Übertragungszeit eine eher unter-

---

[81] Vgl. http://www.nytimes.com/2011/02/26/world/middleeast/26nuke.html?_r=1 (Online-Artikel in der New York Times vom 25. 2. 2011).

[82] Unter Smart Metering versteht man den Einsatz intelligenter Zähler, die den Zweck verfolgen, variable Leistungsentgelte in Abhängigkeit von der Gesamtnachfrage und Netzauslastung erheben zu können und so eine bessere Ausnutzung des Netzes und der vorhandenen Kraftwerkinfrastruktur zu gewährleisten. Die Reaktion des Staates und des Rechtssystems auf diese Innovation steht noch am Anfang. In Deutschland sind Smart Meter keine Pflicht; lediglich bei Neubauten und bei Totalsanierungen müssen gem. § 21b Abs. 3b EnWG ab 2010 intelligente Zähler (für Strom und Gas) kostenneutral eingebaut werden; zum Smart Metering *v. Wege/Sösemann*, IR 2009, 55 ff.; *Eder/v. Wege*, IR 2008, 50 ff.; *Benz*, ZUR 2008, 457 ff.; *Hobbeling/Heine*, CuR 2008, 131 ff.; zu datenschutzrechtlichen Aspekten *Göge/Boers*, ZNER 2009, 370 ff.;

geordnete Rolle, sodass bei Einsatz entsprechender Verschlüsselungs- und Authentifizierungstechniken das Internet als Übertragungsmedium durchaus geeignet ist.

Ganz anders sieht es bei der Fernsteuerung von dezentralen Energieanlagen z. B. in virtuellen Kraftwerken insbesondere bei der Erbringung von Regelleistung aus, die zur Gewährleistung der Netzstabilität unerlässlich ist und innerhalb fester Zeitgrenzen (wenige Sekunden bis Minuten, je nach Stufe) zu erbringen ist. Hier stehen die Übertragungsnetzbetreiber in der Verantwortung, die Stromversorgung durchgängig zu sichern und gegen Sicherheitsbedrohungen zu schützen. Da dabei die Verfügbarkeit von Regelleistung eine Schlüsselrolle einnimmt, gibt es Mindestanforderungen an die einzusetzende Informationstechnik[83], die eine Kommunikation zwischen den Leitsystemen auf Basis des (heutigen) Internets ausschließt und an der Schnittstelle zu den Übertragungsnetzbetreibern den Einsatz eines Internet-Protokolls verbietet. Gründe dafür sind sicherlich die Anforderungen an die Redundanz der Übertragung und ihrer Verfügbarkeit. So sind bspw. zur Erbringung von Sekundärregelleistung zwischen Übertragungsnetzbetreiber und Leistungserbringer zwei separate Übertragungswege mit einer Verfügbarkeit von jeweils mindestens 98,5 % und Latenzzeiten von max. fünf Sekunden auf der gesamten Datenstrecke zu realisieren, wobei die Daten über einen verschlüsselten IPsec-VPN-Tunnel zu übertragen sind – Anforderungen, deren Erfüllung durch das Internet gegenwärtig und auch in naher Zukunft nicht sichergestellt ist, sodass bei hohen Sicherheitsanforderungen auf unabhängige und redundant ausgelegte, hochverfügbare Kommunikationsinfrastrukturen zurückgegriffen werden muss, die nur von einem bekannten Teilnehmerkreis nutzbar sind. Diese Aussagen sind auf andere Versorgungsnetze wie Fernwärme, Gas, Wasser und Abwasser, die ebenfalls kritische Infrastrukturen sind, generell übertragbar, auch wenn IT und Kommunikationsnetze noch keine so zentrale Rolle wie bei der Stromversorgung einnehmen.

Die vom Bundesamt für Sicherheit in der Informationstechnik veröffentlichte technische Richtlinie TR 03109 legt die Anforderungen an die Kommunikationseinheit eines intelligenten Messsystems, des sog. „Smart Meter Gateway“ (SMGW) fest. Dieses soll die Schlüsselrolle bei der Einbindung von Gebäuden mit ihren Verbrauchern und dezentralen Erzeugern in das Smart Grid übernehmen. Trotz der hohen Sicherheitsanforderungen an die Kommunikation z. B. vom Betreiber eines virtuellen Kraftwerks (VK) über das SMGW hin zum Blockheizkraftwerk (BHKW) eines sog. Letztanwenders, ist nicht ausgeschlossen, dass dieses BHKW eine – völlig ungesicherte – Verbindung ins Internet besitzt. Durch einen Angriff über dieses „offene“ Einfallstor könnte in böswilliger Absicht die Hoheit über die Steuerung des BHKW

Raabe, DuD 2010, 379 ff.; *Roßnagel/Jandt*, DuD 2010, 373 ff.; *Karg*, DuD 2010, 365 ff.; *Müller*, DuD 2010, 359 ff.

[83] Z. B. „Mindestanforderungen an die Informationstechnik des Anbieters für die Erbringung von Sekundärregelleistung“ der Übertragungsnetzbetreiber, in der Fassung vom 28. 5. 2013.

übernommen werden. Das könnte u. a. zur Gefährdung der Netzstabilität führen, wenn z. B. das gekaperte BHKW trotz gegenteiligen Signals durch den VK-Betreiber Strom in das Niederspannungsnetz einspeist, obwohl gerade ein Überschuss aus erneuerbaren Energien besteht. Dies könnte sogar gegenüber dem VK-Betreiber durch Übermittlung falscher Statusinformationen über die sichere Datenstrecke via SMGW verschleiert werden. Des Weiteren könnten über die „Hintertür" die schützenswerten Messdaten aus den Zählern der Letztanwender ausgelesen und in unzulässiger Weise publiziert oder missbraucht werden.

3. Gesundheit

Nicht zuletzt bedingt durch die mittlerweile nur noch elektronisch durchzuführende Leistungsabrechnung kann man von einer fast vollständigen IT-Durchdringung von Arztpraxen, Apotheken und Krankenhäusern ausgehen. Dies betrifft nicht nur die eher administrative Leistungserfassung, sondern auch die Verwaltung von medizinischen Daten in lokalen elektronischen Patientenakten sowie den einrichtungsinternen Austausch von Daten zwischen IT-Systemen (z. B. Weiterleitung und Verarbeitung von digitalen Daten aus der Radiologie oder Laborsystemen).

Insbesondere in Krankenhäusern sind zusätzlich jedoch auch noch viele Papierformulare im Einsatz, über die insbesondere die für einzelne Fachbereiche definierten spezifischen Prozesse abgebildet werden. Dies liegt zum einen an den hohen Kosten einer IT-Integration und wird zusätzlich durch mangelnde Interoperabilität zwischen den IT-Systemen befördert, wodurch vor allem in andere Fachbereiche hereinragende Prozessketten oftmals nicht durchgängig elektronisch abgedeckt werden können. Diese Interoperabilitätsprobleme sind in der externen Kommunikation noch akuter und aktuell nur für einzelne Fragestellungen und auch dort oftmals nur proprietär gelöst. Ausnahmen sind „historisch" gewachsene Datensätze (z. B. LDT für die Laborkommunikation), die jedoch auch nur in einzelnen Sektoren (z. B. ambulante Versorgung) gängig sind und bei Weitem nicht von allen Herstellern unterstützt werden.

Bedingt durch diese mangelnde Interoperabilität und nur punktuelle Anforderungen nach einrichtungsübergreifendem Austausch von Patientendaten, sind Kernprozesse der Patientenversorgung von der Verfügbarkeit einer Internetanbindung weitgehend entkoppelt. Viele Arztpraxen verfügen über keinen Internetanschluss oder haben aus Sicherheitsgründen alle Patientendaten haltenden Systeme zwar in einem LAN verbunden, dieses aber strikt von online-fähigen Rechnern separiert. Arztbriefe werden nach wie vor fast vollständig per Post oder über den Patienten ausgetauscht.

Elektronische Kommunikation über das Internet findet lediglich in kleineren regionalen Netzwerken (z. B. Fallakte der städtischen Kliniken München oder teleradiologische Kooperationen) oder in Pilotprojekten (z. B. elektronischer Arztbriefversand in der Region Düren) statt. Hierbei werden zumeist auch nur wenig struktu-

rierte und nur rudimentär semantisch interoperabel kodierte Daten ausgetauscht, sodass der Mehrwert lediglich in der höheren Datenverfügbarkeit liegt, eine maschinelle Weiterverarbeitung jedoch nicht möglich ist. Bei einem Ausfall des Internets wären somit auch diese Kommunikationsstrecken zumindest ohne signifikanten Informationsverlust durch Post oder Fax ersetzbar.

Die einzige relevante Ausnahme hiervon bilden telemedizinische Netzwerke zur Überwachung von Risikopatienten, die zumindest regional und diagnosespezifisch bereits regelhaft zum Einsatz kommen und teilweise auch signifikante Patientenzahlen betreffen. Auch wenn die Daten vom Patienten ausgehend zunächst über Mobilfunkprotokolle übertragen werden, so findet in den meisten Fällen eine Zusammenfassung, Normierung und initiale Auswertung der Daten in einem zentralen Hub (Rechenzentrum) statt, von wo aus die Daten dann über das Internet an das die Patienten betreuende Krankenhaus weitergeleitet werden. Ein Ausfall des Internetzugangs eines Krankenhauses würde hier zusätzliche Risiken für die telemedizinisch betreuten Patienten mit sich bringen und insbesondere auch deren Mobilität und Lebensqualität einschränken.

Die einzelnen Krankenhäuser, Arztpraxen und Apotheken sind darüber hinaus auch Wirtschaftsunternehmen, die in ihren operativen und administrativen Belangen an vielen Stellen auf das Internet angewiesen sind[84]. Neben der Leistungsabrechnung betrifft dies vor allem die Beschaffung von Medikamenten und Verbrauchsgegenständen. Insbesondere bei einer weitgehenden Integration in die Warenwirtschaftssysteme eines Krankenhauses und/oder einer Krankenhausapotheke kann hier durchaus eine kritische Abhängigkeit entstehen, da entsprechende Lieferketten weitgehend automatisiert und elektronisch ablaufen. Dies betrifft gerade multimorbide Patienten, deren Medikation oftmals bereits verblistert angeliefert wird, um Medikationsfehler entlang der Auslieferungskette im Krankenhaus auszuschließen.

Zusammenfassend kann man daher sagen, dass Gesundheitseinrichtungen derzeit nur punktuell von der Verfügbarkeit des Internets abhängig sind, diese Abhängigkeit jedoch gerade Risikopatienten betrifft. Ein Ausfall des Internetzugangs würde so zwar nur wenige Patienten betreffen, für diese jedoch mit signifikanten Risiken einhergehen. Zusätzlich ist davon auszugehen, dass mit den zunehmenden telemedizinischen Versorgungsdiensten, diese Risiken in Zukunft tendenziell ansteigen werden.

---

[84] Allgemein zur Abhängigkeit von Gesellschaft, Wirtschaft und Verwaltung vom Internet *Schulz* (Fn. 75), S. 265 (269 ff.).

4. Öffentliche Sicherheit am Beispiel des Katastrophenschutzes

Abschließend wurde für die exemplarische Betrachtung ein Bereich ausgewählt, der aufgrund seiner Kritikalität und der besonderen Anforderungen in Krisenfällen eigentlich kaum Abhängigkeiten vom Internet aufweisen dürfte. Allerdings zeigen sich erstaunlicherweise auch hier in einigen Bereichen potenzielle Risiken.

Der Katastrophenschutz ist in Deutschland föderal organisiert und liegt im Verantwortungsbereich der Länder bzw. der kreisfreien Städte und Landkreise, während der Zivilschutz im Verteidigungsfall im Verantwortungsbereich des Bundes liegt[85]. Durch die Verteilung der Kompetenzen und die unterschiedlichen Anforderungen sind die Prozesse sowie die eingesetzten Systeme dementsprechend heterogen. Auf allgemeiner Ebene werden daher folgende generelle Bereiche betrachtet:

a) Interne Prozesse und Kommunikation der Katastrophenschutzbehörden

In dem direkten Bereich der Kommunikation und des Datenaustausches zwischen Leitstellen und Lagezentren verfügen die Katastrophenschutzbehörden über eigene vom Internet getrennte Netze, die per Kabel, Richtfunk oder Satellit realisiert sind. In der Regel sind diese Netze IP-basiert und bieten daher über Updates der Router-Software und die internen Server grundsätzlich Angriffsflächen, die bspw. durch das unbewusste Einspielen von fehlerhaften und schädlichen Codes bei Wartungsprozessen zu späteren Ausfällen im Ernstfall führen können. Grundsätzlich hat auch die physische Vulnerabilität dieser Verbindungen gegenüber früheren einfachen, analogen Kupferkabelverbindungen zugenommen. Bspw. erfordert die verwendete Internet-Technologie auch bei der Wiederherstellung in Krisensituationen weitaus mehr Know-how und komplexere Hardware-Komponenten, die im schlimmsten Fall nicht mehr zur Verfügung stehen.

b) Prozesse zwischen Katastrophenschutzbehörden und weiteren Behörden sowie kritischen Infrastrukturbetreibern

In der Regel gibt es hier keine dedizierten, vom Internet getrennten Netze, die die Katastrophenschutzbehörden mit anderen Behörden und kritischen Infrastrukturbetreibern verbinden. Im Bereich der Kommunikation existieren durch den Wegfall des analogen Telefonnetzes in diesem Fall auch keine klassischen Sprachverbindungen als Rückfallebene, die unabhängig vom Internet sind. Derzeit besteht damit im Krisenfall nur die Möglichkeit, Kommunikationsverbindungen zu kritischen Infrastrukturen wie Krankenhäusern, Energie- oder Wasserversorgern per Funk (in Zu-

---

[85] Gem. Art. 30 i. V. m. Art. 70 Abs. 1 GG; zur Reichweite der Bundeskompetenz beim Zivilschutz *Heintzen,* in: v. Mangoldt/Klein/Starck (Hrsg.), GG, Bd. 2, 6. Aufl. 2010, Art. 73 Rn. 19 ff. Der Bund übernimmt jedoch in zunehmenden Maße über das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe übergreifend koordinierende Aufgaben auch außerhalb des Zivilschutzes.

kunft per digitalem BOS[86]) über mobile Einsatzfahrzeuge zu improvisieren, soweit zu diesen keine dedizierten Funk- oder Kabelverbindungen bestehen. Diese Verbindungen sind dann allerdings nicht (Analogfunk) oder nur äußerst begrenzt (digitaler BOS) zur Datenübertragung geeignet. Mit dem künftig zunehmenden Bedarf an Vernetzung und Datenaustausch zur Erfassung von komplexen Lagen im Lagebild und koordinierten Gefahrenabwehrprozessen mit Dritten ist auch eine Vernetzung dieser Akteure erforderlich. Diese notwendige Vernetzung wird mit erheblichen Kosten verbunden sein, da diese aus den genannten Gründen nicht über das Internet, sondern nur über eigene dedizierte Netze realisiert werden kann.

c) Prozesse zwischen Katastrophenschutzbehörden und Einsatzkräften sowie Bevölkerung

In diesem Bereich sind die wesentlichen Abhängigkeiten vom Internet identifizierbar. So ist bspw. im digitalen BOS keine Sicherstellung der Alarmierung der Rund 450.000 Freiwilligen vorgesehen. Diese werden daher weiterhin per Analogfunk, über das Funkrufprotokoll POCSAG oder per SMS alarmiert. Aufgrund der hohen Kosten für Endgeräte nimmt die SMS-Alarmierung hier einen immer größeren Anteil ein. Neben dem hier nicht untersuchten Einfluss eines möglichen flächendeckenden und länger anhaltenden Ausfalls des Internets auf die Funktion des Mobilfunknetzes stellt allein die Verbindung der per Internet realisierten Anschlüsse der SMS-Alarmierungssoftware in der Leitstelle zu den SMS-Providern ein essenzielles Risiko dar. Zusätzlich wird die SMS derzeit auf Smartphones verstärkt durch kostenfreie internetbasierte Push-Dienste wie Apple- und Google-Notification ersetzt.

Dieses Problem betrifft auch die Warnung und Information der Bevölkerung in Katastrophenfällen. Zwar verfügt das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) mit SatWaS (Satellitengestütztes Warnsystem) eine Satellitengestützte Verbindung zu wichtigen TV- und Radio-Stationen zur Verbreitung von Warninformationen, die mit der Ausbaustufe MoWaS (Modulares Warnsystem) auch den Ländern zugänglich gemacht wurde. Das veränderte Medienkonsumverhalten und die zunehmende Verlagerung von Medieninhalten auf das Internet vermindert jedoch zunehmend die Effektivität dieses Informationskanals. Zusätzliche Warnkanäle per Mobilfunk sind zwar realisiert, jedoch auch weitestgehend von der Funktion des Internets abhängig. Unabhängige Techniken wie Cell-Broadcast sind mit größeren technischen Problemen und hohen Kosten verbunden und bieten gerade im Bereich erweiterter Warndienste wie Gefahrenkarten, Verhaltenshinweisen und Rückmeldungen keine Zukunftsfähigkeit.

Auch der Bereich des Notrufs ist mit dem sukzessiven Wegfall des analogen Telefonnetzes – jenseits des Aspekts der Stromabhängigkeit der nunmehr digitalen

[86] Digitaler Behördenfunk.

Telefonie – zumindest bei VoIP-Anschlüssen vom Internet abhängig, darüber hinaus u. U. zumindest mittelbar betroffen. Gerade in dem in Zukunft zentralen Bereich der Kommunikation mit der Bevölkerung in Krisensituationen sind die wichtigsten Kommunikationskanäle direkt oder indirekt vom Internet abhängig, sodass hier von einem erheblichen Bedrohungsrisiko ausgegangen werden muss.

G. Handlungsfelder

Die beschriebenen Abhängigkeiten, Szenarien und die z. T. als defizitär identifizierten Zustände bei gleichzeitiger Qualifikation von IT-Systemen als „kritisch“ im Sinne der gefundenen Definition zeigen einen deutlichen Handlungsbedarf. Im Folgenden soll daher erläutert werden, wie im Bereich der Handlungsfelder „Regulierung“ (I.), „Technik“ (II.) und „Organisationskultur“ (III.) auf diesen Befund reagiert werden kann.

I. Regulierung

Handlungsinstrumente und damit auch der rechtliche Rahmen werden im Bereich kritischer Infrastrukturen und im Sinne einer Risikominimierung klassischerweise in Präventions-, Detektions- und Reaktionsmaßnahmen aufgegliedert. Schwerpunkt soll für den regulatorischen Ansatz die Prävention sein, da die Detektion im Kontext von IT technisch diffizile Vorgänge beschreibt, die ihrerseits rechtlich – mit der Ausnahme einer Meldepflicht für erkannte Beeinträchtigungen und „Angriffe“[87] – kaum determinierbar sind und die Reaktion im Bereich des Zivil- und Katastrophenschutzes angesiedelt ist. Die vorgenannten Differenzierungen führen dazu, dass sich auch der zur Absicherung ggf. erforderliche Rechtsrahmen aus verschiedenen Elementen zusammensetzt.

1. hinsichtlich der „anderen“ kritischen Infrastrukturen

So existieren für die kritischen Infrastrukturen ihrerseits bestimmte rechtliche Vorgaben, bspw. was die Vorhaltung von redundanten Systemen, Zugangssicherungen, Notfall- und Krisenmanagement betrifft. Exemplarisch kann etwa § 6 PTSG[88] genannt werden, der eine Telekommunikationsbevorrechtigung (also die unverzügliche und vorrangige Bereitstellung und Entstörung von Anschlüssen und Übertragungswegen sowie die vorrangige Herstellung von Verbindungen im Mobilfunk) für diverse öffentliche Stellen sowie ausdrücklich für Katastrophenschutz-, Zivilschutz- und Hilfsorganisationen, Aufgabenträger im Gesundheitswesen und Hilfs- und Rettungsdienste vorsieht. Auch Notrufverbindungen i. S. v. § 108 TKG sind vorrangig herzustellen.

---

87 So vorgesehen im IT-SIG-E (Art. 1 § 8b Abs. 2): „Das Bundesamt hat (…) die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen, insbesondere zu (…) erfolgten und versuchten Angriffen auf die Sicherheit in der Informationstechnik zu sammeln und auszuwerten (…)“.

88 Gesetz zur Sicherstellung von Postdienstleistungen und Telekommunikationsdiensten in besonderen Fällen vom 24. 3. 2011, BGBl. I S. 506.

2. hinsichtlich der IT-Sicherheit (der kritischen IT-Systeme) anderer kritischer Infrastrukturen

Aufgrund der zunehmenden Bedeutung der IT und neuer Bedrohungsszenarien, die einen Zugriff auf andere kritische Infrastrukturen über die eingesetzte IT weitaus einfacher erscheinen lassen als bspw. klassische Sabotageakte, wird dieser Rechtsrahmen zunehmend ergänzt bzw. ergänzt werden müssen um Regelungen, die speziell die IT-Sicherheit – nicht allgemein, sondern diejenige der kritischen Infrastrukturen – adressieren[89]. Der präventive Schutz kritischer IT-Infrastrukturen ist dem Recht der IT-Sicherheit zuzuordnen[90]. Hierbei handelt es sich um eine heterogene Rechtsmaterie, die sowohl öffentlich-rechtliche als auch zivilrechtliche Normen mit unterschiedlichem Regelungsgehalt umfasst, deren gemeinsamer Nenner die Gewährleistung von Sicherheit in der Informationstechnik ist[91]. Speziell auf die IT-Systeme der kritischen Infrastruktur zielt der Entwurf eines IT-Sicherheitsgesetzes, der für die Betreiber kritischer Infrastrukturen einschließlich der Telekommunikationsdiensteanbieter, also gerade private Akteure, die Einhaltung eines Mindestniveaus an IT-Sicherheit vorsieht. Hinzu kommt eine den Betreibern auferlegte Meldepflicht sicherheitsrelevanter Vorkommnisse an das Bundesamt für Sicherheit in der Informationstechnik, welches wiederum die Verpflichteten verstärkt berät und unterstützt.

Daneben existieren auch bereichsspezifische Vorgaben für die IT-Sicherheit: Zu diesen sind insbesondere § 109 TKG, § 25a KWG[92], § 9 BDSG und § 13 TMG zu zählen. § 25a KWG macht bankenaufsichtsrechtliche Vorgaben für die beaufsichtigten Kredit- und Finanzdienstleistungsinstitute: Als Bestandteil des institutsinternen Risikomanagements wird durch § 25a Abs. 1 Satz 3 Nr. 3 KWG auch die die Festlegung eines angemessenen Notfallkonzepts, insbesondere für IT-Systeme, verpflichtend vorgesehen. § 9 BDSG normiert für alle Bereiche der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten das Erfordernis, technische und organisatorische Maßnahmen zu treffen, um den Anforderungen des Datenschutzes zu genügen. Dazu gehört insbesondere die Sicherstellung eines ordnungsgemäßen Ablaufs der Datenverarbeitung, indem Hard- und Software gesichert werden und die Daten vor Verlust, Beschädigung, Missbrauch, Diebstahl und Verfälschung geschützt werden[93]. Auch § 13 TMG verpflichtet die Anbieter von Telemediendiensten, technische und organisatorische Vorkehrungen zu treffen, die einen sog. Systemdatenschutz, also die Ausgestaltung technischer Systeme dahingehend, dass sie nur noch zu der Datenverarbeitung in der Lage sind, zu der sie rechtlich ermächtigt

---

89 *Schulz/Tischer,* ZG 2013, 339 (353).

90 *Gaycken/Karger*, MMR 2011, 3 (6).

91 *Gaycken/Karger*, MMR 2011, 3 (6).

92 Gesetz über das Kreditwesen i. d. F. d. Bek. vom 9. 9. 1998, BGBl. I S. 2776.

93 *Spindler*, in: Kloepfer (Fn. 10), S. 85 (94), m. w. N.

sind, und die verantwortliche Stelle nur noch die Daten verarbeitet, die sie rechtlich verarbeiten darf[94], gewährleisten. Art. 3 IT-SIG-E sieht die Erweiterung der Vorschrift um die zusätzliche Verpflichtung zu entsprechenden Vorkehrungen und Maßnahmen gegen unerlaubten Zugriff vor.

3. hinsichtlich „des Internets" und der IT-Sicherheit der kritischen IT-Systeme

Neu hinzutreten muss – soweit die rechtlichen und diesen folgend tatsächlichen Maßnahmen, die zur Absicherung der Telekommunikationsinfrastrukturen ergriffen werden, nicht ausreichen – ein spezielles Rechtsregime, welches „das Internet" als kritische Infrastruktur zum Regelungsgegenstand hat[95]. Da das Internet weitgehend auf den Telekommunikationsinfrastrukturen basiert, mittlerweile sogar deren primäre Funktion sein dürfte, da sich auch die herkömmlichen Kommunikationsdienste (Telefon, Fax usw.) zunehmend auf die dem Internet zugrunde liegende IP-Technologie verlagern, ist Anknüpfungspunkt auch der kritischen Infrastruktur „Internet" das TKG. Dies wird auch im Kontext des IT-SIG deutlich herausgestellt: „Die TK- und Telemediendiensteanbieter, die eine Schlüsselrolle für die Sicherheit des Cyber-Raums haben, werden stärker als bisher hierfür in die Verantwortung genommen"[96].

Gemäß § 109 TKG hat der Diensteanbieter angemessene technische Vorkehrungen oder sonstige Maßnahmen zu treffen, um die im Gesetz genannten Schutzgüter zu schützen[97]. Als technische Vorkehrungen sind alle Maßnahmen zu verstehen, die sich auf die Funktionsweise der technischen Einrichtung beziehen. Bei der Planung sind sämtliche in Betracht kommende Risiken einzubeziehen[98]. Nach § 109 Abs. 2 Satz 4 TKG sind die Vorkehrungen und Maßnahmen angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand in einem angemessenen Verhältnis zur Bedeutung der zu schützenden Rechte und zur Bedeutung der zu schützenden Einrichtungen für die Allgemeinheit steht. Zwischen dem Aufwand, den der Verpflichtete zu treffen hat, und dem Nutzen für die Allgemeinheit darf kein Missverhältnis bestehen[99]. Welche Schutzmaßnahmen angemessen sind, muss anhand des Einzelfalls entschieden werden; hierbei ist der Stand der technischen

---

94 *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Auflage 2011, § 13 TMG Rn. 8.

95 *Schulz/Tischer,* ZG 2013, 339 (354).

96 *Friedrich*, MMR 2013, 273 (274).

97 Siehe zum Folgenden *Gaycken/Karger,* MMR 2011, 3 (6).

98 *Eckhardt*, in: Geppert/Schütz (Hrsg.), Beck'scher TKG-Kommentar, 4. Aufl. 2013, § 109 Rn. 27.

99 *Eckhardt* (Fn. 98), § 109 Rn. 46.

Entwicklung relevant[100]. Zu berücksichtigen ist weiter, dass es eine absolute Sicherheit nicht geben kann und eine extrem hohe Sicherheit für die Allgemeinheit oft nicht bezahlbar ist[101]. Allerdings dürfen Sicherheitsanforderungen nicht alleine an Rentabilitäts- oder Wirtschaftlichkeitsbetrachtungen festgemacht werden. Zu den bislang üblichen und als angemessen betrachteten technischen Vorkehrungen zählen Firewalls, Überbrückungsaggregate, der Betrieb redundanter Systeme sowie die Überwachung des eigenen Netzes mit Hilfe von Intrusion-Detection-Systemen[102].

Dieser Rechtsrahmen sichert zwar einen wesentlichen Teil der für das Internet erforderlichen Infrastruktur ab, es wurde jedoch bereits darauf hingewiesen, dass wichtige Elemente existieren, die weder vom TKG noch von anderen Regulierungen erfasst werden. Die erforderliche Regulierung erschöpft sich nicht lediglich in der IT-Sicherheit – so ist es Zielsetzung des IT-SIG-E, diese Anforderungen auch auf nicht-regulierte Bereiche auszudehnen –, sondern muss ggf. darüber hinausgehen, da die Bedrohungen nicht nur von dritter Seite (vor denen IT-Sicherheit schützen soll), sondern auch von Betreiberseite selbst ausgehen können. Eine „Betriebspflicht" für bestimmte – bisher auf Freiwilligkeit und Selbstregulierung basierende – Systeme wäre zumindest zu diskutieren.

Indem der Staat durch den Abbau des Monopols im Telekommunikationsbereich auch seinen unmittelbaren Einfluss auf diese kritische Infrastruktur aufgegeben hat, ist zu deren Schutz eine sachgerechte Verantwortungsteilung[103] von Staat und Unternehmen erforderlich. Diese macht den Schutz kritischer Infrastrukturen zu deren gemeinsamer Aufgabe, bei deren Erfüllung der Ausgleich zwischen Wirtschafts- und übergeordneten Allgemeininteressen herzustellen ist. Eine etwaige Übergewichtung des wirtschaftlichen Interesses seitens der über mehr Einfluss verfügenden Betreiber könnte allerdings den fragilen Ausgleich stören und zu Unzulänglichkeiten beim Schutzniveau führen. Deshalb ist zur Sicherstellung des Gemeinwohls auch die Auferlegung bestimmter Pflichten denkbar. Die Rechtfertigungsgründe für eine solche Inhalts- und Schrankenbestimmung zu Lasten des Eigentums der Betreiber sind im Kontext der Sozialbindung des Eigentums (Art. 14 Abs. 2 GG) sowie den Anforderungen, die eine Enteignung rechtfertigen würden, zu sehen: Eine Enteignung erforderte ein besonders schwerwiegendes, dringendes öffentliches Interesse[104]. Die bei einem Ausfall des Internets denkbaren Szenari-

---

100 *Spindler* (Fn. 93), S. 85 (90).

101 *Eckhardt* (Fn. 98), § 109 Rn. 46.

102 *Eckhardt* (Fn. 98), § 109 Rn. 46; *Spindler* (Fn. 93), S. 85 (91 f.).

103 S. Gliederungspunkt C. III. sowie zum Ganzen *Kloepfer* (Fn. 13), S. 9 (17).

104 Statt vieler nur *Axer*, in: Epping/Hillgruber (Hrsg.), Beck'scher Online-Kommentar GG, Ed. 18 (Stand: 15. 5. 2013), Art. 14 Rn. 116.

en[105] lassen das Vorliegen selbst dieser vergleichsweise engen Voraussetzung nicht von vornherein ausgeschlossen erscheinen. Für kritische Infrastrukturen im Allgemeinen ist an deren Definition zu erinnern, die mit den Anforderungen an eine Enteignung vergleichbare Merkmale aufweist: Es handele sich um Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe bis hin zu Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten können[106]. Das Auferlegen bestimmter Betriebs- und Sicherungspflichten, um solchen Risiken vorzubeugen, erscheint gegenüber der Enteignung allerdings als wesentlich milderes Mittel. Es dürfte vor den Rechtfertigungsanforderungen einer Inhalts- und Schrankenbestimmung angesichts des hohen Gemeinwohlinteresses einer Aufrechterhaltung bestimmter Dienste fraglos Bestand haben[107].

II. Technik

Die Handlungsinstrumente bezüglich der technischen Sicherheit gliedern sich in zwei unterschiedliche Perspektiven. Der Schutz des Internets an sich ist sowohl eine regulatorische Aufgabe als auch eine technische. Das individuelle Gestaltungspotenzial der Internetnutzer hinsichtlich der technischen Struktur des Internets ist jedoch beschränkt. Die Auswahl der Protokolle und technischen Verfahren sowie der Zuordnung von Namen und Nummern werden im Rahmen der IETF[108] bzw. der IANA[109] vorgenommen. Insbesondere über eine Beteiligung an der Arbeit der IETF zu Vorschlägen für die Internet-Standardisierung können auch deutsche Unternehmen und Behörden ihre Interessen in Bezug auf die technische Absicherung des Internets einbringen.

Betrachtet man die Handlungsspielräume von Infrastrukturbetreibern, die das Internet als Kommunikationsinfrastruktur für ihre eigene Infrastruktur verwenden, so gliedern sich auch die technischen Handlungsinstrumente typischerweise in die Bereiche Prävention, Detektion und Reaktion.

---

105 Vgl. oben Gliederungspunkt F.

106 Oben Fn. 9.

107 *Schulz/Tischer,* ZG 2013, 339 (356).

108 Die Internet Engineering Task Force (IETF) ist eine Aktivität der Internet Society (ISOC) und basiert auf der Zusammenarbeit von freiwilligen Experten, die meist durch ihre Arbeitgeber unterstützt werden.

109 Die Internet Assigned Numbers Authority (IANA) ist eine Abteilung der Internet Corporation for Assigned Names and Numbers (ICANN), eine zivilrechtliche Non-Profit-Organisation mit Sitz in Kalifornien.

1. Vorbeugen (Prävention)

Technische Maßnahmen zum präventiven Schutz kritischer Systeme und Infrastrukturen lassen sich grob in die zwei Bereiche „Realisierung technischer Sicherheits- oder Gegenmaßnahmen“ sowie „Qualitätssicherung“ aufteilen.

Bei der Realisierung technischer Sicherheits- oder Gegenmaßnahmen geht es darum, Risiken, die im Rahmen einer Risiko- und Bedrohungsanalyse als relevante Bedrohung identifiziert worden sind, durch das Einbringen technischer Maßnahmen zu reduzieren. Der Katalog solcher technischer Maßnahmen aber ist lang und hängt stark vom betrachteten technischen System bzw. der betrachteten Infrastruktur ab. Er reicht von der Einführung sicherer Software, sicherer Protokolle und kryptographischer Verfahren, geht über die redundante Auslegung kritischer Systeme und Subsysteme, um Ausfallsicherheit zu erlangen, und reicht bis hin zur logischen oder physikalischen Abschottung kritischer Systembereiche.

Wichtig bei der Einführung neuer Mechanismen ist das grundsätzliche Verständnis des Designs von Internet-Protokollen und der Internet-Strukturmerkmale, wie sie schon oben in Gliederungspunkt D. II. dargestellt wurden. Ein Negativbeispiel ist die Sperrung von Webseiten basierend auf dem Domain Name System, wie es bspw. nach dem Zugangserschwerungsgesetz[110] geplant war. Abgesehen von der rechtlichen Bewertung wurde in der sog. Stoppschild-Debatte schnell die technische Wirkungslosigkeit dieser Maßnahme bekannt.

Qualitätssicherungsmaßnahmen stellen darüber hinaus sicher, dass die Systeme zuverlässig ihre Funktionalität erbringen und die eingebrachten Gegenmaßnahmen wirksam sind. Zu den gängigen Qualitätssicherungsmaßnahmen gehören formale Verifikation, Testen und die Durchführung von Reviews.

Für die Bereiche Betriebssicherheit und IT-Sicherheit gibt es eine Reihe von Leitlinien, die für einzelne Anwendungsbereiche Vorgaben an die Realisierung technischer Sicherheits- oder Gegenmaßnahmen sowie ihre Qualitätssicherung machen.

Für den Bereich der Betriebssicherheit ist das u. a. die ISO 61508, aus der sich weitere anwendungsgebietsspezifische Normen u. a. für die Prozesstechnik, Kernkraftwerke, Bahnanwendungen, medizinische Geräte und Straßenfahrzeuge ableiten. Der Geltungsbereich der Norm erstreckt sich über Planung, Entwicklung, Realisierung, Inbetriebnahme und Betrieb bis hin zur Außerbetriebsetzung sowohl des gefahrverursachenden Systems wie auch der sicherheitsbezogenen Systeme und Gegenmaßnahmen.

---

[110] Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen vom 17. 2. 2010, BGBl I S. 78, aufgehoben mit Wirkung vom 29. 12. 2011 durch Gesetz vom 22. 12. 2011, BGBl I S. 2958.

Ähnlich wie im Umfeld der Betriebssicherheit gibt es auch für den Bereich der IT-Sicherheit Schemata, mit denen sich Geräte in Bezug auf ihre IT-Sicherheit begutachten lassen. Ein solches Zertifzierungsschema sind die Common Criteria for Information Technology Security Evaluation (CC, ISO/IEC 15408)[111]. Der ISO-Standard ist abgeleitet von bekannten internationalen Standards wie dem Orange Book (1985), ITSEC (1991) und der Canadian Criteria (1993). Die aktuelle Version ist Version 3.1, Rev. 4 vom September 2012. Erklärtes Ziel der CC ist es, eine Basis für die Evaluierung der IT-Sicherheitsfunktionalität zu definieren, die eine Vergleichbarkeit der Auswertungsergebnisse gewährleistet. Dies wird über eine gemeinsame standardisierte Methodik, die Common Methodology for Information Technology Security Evaluation (ISO/IEC 18045)[112], gewährleistet. Die Methodik ist Teil der internationalen Anerkennung nationaler Evaluierungsergebnisse, die im Common Criteria Recognition Arrangement (CCRA) vereinbart ist. In Deutschland ist das Bundesamt für Sicherheit in der Informationstechnik für Zertifizierungen nach den CC verantwortlich. Zusätzlich dazu definiert die ISO/IEC 27000-Familie eine Sammlung von Standards, die eine einheitliche Terminologie und die Definition einheitlicher (standardisierter) Kriterien enthalten, nach welchen Organisationen hinsichtlich ihrer Aktivitäten zur Gewährleistung der Informationssicherheit bewertet werden können[113].

2. Erkennen (Detektion)

Aufgrund der Komplexität der technischen Systeme werden immer Sicherheitslücken oder Systemschwächen vorhanden sein, die zu Angriffen auf kritische Infrastrukturen ausgenutzt werden können oder deren Funktionsfähigkeit schwächen. Daher ist die – möglichst frühzeitige – Erkennung von (durch Vorbeugung nicht vollständig vermeidbaren) Problemen ein weiteres, wichtiges Handlungsfeld.

Anwendungen basieren normalerweise auf einer Reihe von Komponenten, die als Funktionsbausteine so zusammengestellt werden, dass sie die Gesamtfunktion der Anwendung erbringen. Bspw. könnte eine Anwendung „Datenspeicher“ vereinfacht aus den Funktionen „Benutzeridentifikation“, „Datenübertragung“ und „Datenspeicherung“ bestehen. Die Verfügbarkeit der Anwendung ist nur gegeben, wenn alle Einzelfunktionen verfügbar sind, die durchaus von verschiedenen Plattformen und Anbietern stammen und von weiteren Faktoren abhängig sein können. Bei den Kommunikationsfunktionen, die bei dieser Betrachtung im Mittelpunkt stehen,

---

[111] Common Criteria for Information Technology Security Evaluation, Version 3.1R4, September 2012.

[112] Common Methodology for Information Technology Security Evaluation, Version 3.1R3, July 2009.

[113] http://de.wikipedia.org/wiki/ISO/IEC_27000-Reihe.

handelt es sich um sehr grundlegende Funktionen, deren Einfluss oft nicht sofort augenfällig ist. Die Abhängigkeiten werden sich nur durch Analysewerkzeuge aufdecken lassen bzw. bedürfen der Erfahrung von gut ausgebildeten System- und Netzwerkadministratoren. So werden bspw. Analysen zum Wachstum des Übertragungsvolumens durchgeführt, um, insbesondere bei Mobilfunknetzen, potenzielle Kommunikationsengpässe frühzeitig erkennen zu können. Das ermöglicht die Planung des Zeitpunkts zum Ausbau der entsprechenden Netze oder Netzkomponenten: Nähert sich ein IP-basiertes Netz seiner Kapazitätsgrenze, so verschlechtert sich die Übertragungsqualität, hingegen sind Überkapazitäten nicht wirtschaftlich.

Für die Erkennung von Problemen (Angriffe, aber auch betriebliche Störungen) müssen die normalen Betriebsparameter mit Hilfe von Monitoring-Werkzeugen erfasst werden. Eine Störung wird als Unterschied zum Normalbetrieb erkannt. Schwierigkeiten bereitet dabei die im Normalbetrieb durchaus auftretende Dynamik, bspw. die Nutzung der Infrastruktur zu verschiedenen Tageszeiten. Auch außergewöhnliche Ereignisse können zu einem starken Anstieg der Nutzung bestimmter Dienste führen[114], sodass der Unterschied zu einem böswilligen Angriff (hier: Denial-of-Service-Attacke) hierbei fließend ist. Zur besseren Unterscheidung der Betriebszustände können verschiedene Parameter miteinander korreliert werden. Im Netzbereich können z. B. Signalisierungsnachrichten betrachtet werden: Werden immer wieder neue Kommunikationsverbindungen aufgebaut, ohne sie anschließend zu nutzen, so kann von einem Angriff ausgegangen werden. In realen Umgebungen sind diese Zusammenhänge wesentlich komplexer und können nur mit Hilfe von technischen Systemen (bspw. selbstlernende Systeme) analysiert werden.

Eine weitere Maßnahme zur Erkennung von Angriffen ist ein sog. Honeypot. Es handelt sich dabei meist um eine Gruppe von Sensoren, die netzseitig IT-Systeme einer bestimmten Funktionsklasse (bspw. PC, Server, aber auch Industriesteuerung) nachbilden und dazu dienen, Angriffe auf diese Sensoren zu erkennen[115]. Dahinter steckt die Erfahrung, dass viele Angriffe automatisiert durchgeführt werden und dabei aktuelle Hard- und Software-Schwachstellen von bestimmten Gerätetypen gezielt ausgenutzt und dazu passende Geräte automatisiert gesucht werden. Mit Hilfe von Honeypots wird es so möglich, sich unabhängig von einer konkreten (durch die Angriffe dann auch gefährdeten) Infrastruktur einen Überblick über aktuelle Angriffe zu verschaffen und diese in Form, Umfang und möglicherweise Herkunft in einer kontrollierten Umgebung zu untersuchen. Schlussendlich hat sich im Internet selber eine Serviceinfrastruktur entwickelt, die sich darauf spezialisiert

---

[114] So kann die Erwähnung von Webseiten kleinerer Projekte in der IT-Berichterstattung zur Problemen der Verfügbarkeit führen, sodass diese nach der Veröffentlichung des Bericht zeitweise nicht mehr verfügbar sind, s. auch http://de.wikipedia.org/wiki/Slashdot-Effekt.

[115] Beispiel: Sicherheitstacho der Deutschen Telekom AG, http://www.sicherheitstacho.eu/.

hat, aktive Bedrohungen im Internet zu identifizieren und Informationen über die Bedrohungen zur Verfügung zu stellen. Genannt werden kann hier Internet Strom Center[116] des SANS Instituts und speziell für Deutschland die Lageberichte und Warnmeldungen des Bundesamts für Sicherheit in der Informationstechnik bzw. der Allianz für Cyber-Sicherheit[117]. Grundsätzlich erscheint es sinnvoll, Messungen und Beobachtungen auf den verschiedenen Ebenen, d. h. Monitoring der Betriebsparameter, Monitoring von Angriffsversuchen (z. B. über Honeypots) und Lagebilder bzw. Warnmeldungen, miteinander zu korrelieren, um die immanenten Unsicherheiten bei der Erkennung von Angriffen reduzieren zu können.

3. Reagieren (Reaktion)

Nach der Erkennung einer Störung oder eines Angriffes ist die Reaktion der nachfolgende logische Schritt. Nach derzeitigem Stand ergeben sich unterschiedliche Strategien für die beiden Bereiche. Bei Störungen steht oft der physische Ausfall einer Ressource im Vordergrund, der durch redundante Systeme und damit eine Systemausweitung abgefangen werden kann. Das Erkennen von Angriffen ist schwieriger und es wird in vielen Fällen versucht, mit gezielten Systembeschränkungen zu reagieren.

Das Erkennen und Reagieren auf Fehler ist ein Bereich des klassischen Netzwerkmanagements, bspw. im FCAPS-Modell[118] das Fault-Management. Der klassische Fall in diesem Bereich ist der Ausfall einer Komponente, bspw. eines Übertragungswegs. Dieser Ausfall wird vom Netzwerkmanagement erkannt und es wird möglichst automatisiert ein Ersatz bereitgestellt, bspw. ein neuer Übertragungskanal bei Ausfall einer Glasfaserstrecke. In vielen Fällen wird der Ausfall von Komponenten schon von einem Lastmanagement-System abgefangen: Wird bspw. die Last von eingehenden Web-Anfragen auf verschiedene Webserver-Instanzen verteilt, so wird beim Ausfall einer Webserver-Instanz diese durch die Lastverteiler-Komponente nicht mehr angesprochen und trotzdem ist nahtloser Betrieb über die verbliebenden Instanzen automatisch gewährleistet. Während des laufenden Betriebs kann dann auch die fehlende Ressource ersetzt werden. Durch die weitergehend zustandslose[119] Verarbeitung von IP-basierter Kommunikation auf dem Übertragungsweg lassen sich auch hier vergleichsweise einfach redundante Systeme

---

116 http://isc.sans.org/.

117 https://www.allianz-fuer-cybersicherheit.de/.

118 http://en.wikipedia.org/wiki/FCAPS.

119 Es werden keine Informationen über eine Verbindung in Netzwerkkomponenten gespeichert, die im Fehlerfall verloren gehen könnten oder auf eine andere Komponente übertragen werden müssten.

aufbauen (bspw. Firewalls), die gleichzeitig für Last- und Fehlermanagement zur Verfügung stehen.

Ein Angriff geht meist mit sinnloser Kommunikation einher. Nur sehr große Infrastrukturen können diese Angriffe über bestehende oder ad-hoc erweiterte Ressourcen abfangen (was auch mit Kosten verbunden ist). Da Angriffe über Bot-Netze einen großen Umfang haben können, versucht man durch Verwendung von Intrusion-Prevention-Systemen dynamisch auf Angriffe zu reagieren. Bspw. kann man Filterregeln bilden, mit denen Anfragen aus einzelnen Netzbereichen des Internets abgeblockt werden, da diese vermeintlich von dem Angriff stammen. Problematisch ist dabei, dass nur schwer zwischen legitimem und illegitimem Datenverkehr unterschieden werden kann, bspw. zwischen tatsächlichen Kunden eines Webshops und dem Verkehr von Angreifern. Somit wird die Reaktion auf den Angriff auch (ahnungslose) Kunden treffen und verärgern. Üblich ist auch, dass eine statische Webseite mit einer Fehlermeldung bereitgestellt wird, deren Auslieferung wesentlich weniger Ressourcen braucht als bspw. die Erzeugung von dynamischen Webseiten. Trotz dieser Maßnahmen werden durch den Angriff noch Ressourcen mit sinnlosem Verkehr belastet, sodass das Ziel sein muss, die Filterung möglichst früh im Kommunikationspfad, in Richtung der Quelle des Angriffs, vorzunehmen. Dieser Ansatz stößt aber durch die Dezentralität des Internets und die Infektion von vermeintlich harmlosen, breit verteilten PC, mit der sie Teil von Bot-Netzen werden, an ihre Grenzen.

III. Organisationskultur

Als drittes Handlungsfeld neben Regulierung und Technik muss die Organisation bzw. Organisationskultur genannt werden, die maßgeblich zum Betrieb und Schutz kritischer Infrastrukturen beiträgt. Im Folgenden soll erörtert werden, wie die Etablierung achtsamer Organisationskulturen dazu beitragen kann, dass wichtige Systeme sicher und nachhaltig betrieben werden können und dabei noch Mehrwert generiert werden kann.

1. Organisationale Achtsamkeit und sichere IT-Systeme als notwendige Voraussetzung für den Schutz kritischer IT-Infrastruktur

Die Betriebsfähigkeit von Organisationen wie Unternehmen und Behörden wird durch immer komplexer miteinander verbundene Systeme sichergestellt. Bei diesen Systemen handelt es sich um vernetzte IT-Systeme, organisationale Systeme und die wiederum daraus entstehende Interaktion dieser beider Systemwelten. Organisationen lassen sich also als ein System von Systemen begreifen, die unterschiedlich alt, zuverlässig, formalisiert und leistungsfähig sind und die u. U. Ergebnisse generieren, die so nicht erwünscht oder vorhersehbar waren. Erhöht man also etwa die regulatorischen Anforderungen an schützenswerte IT-Systeme, ohne jedoch den organisationalen Kontext zu berücksichtigen, innerhalb dessen diese Systeme funktionieren, so wird man kaum zur gewünschten Verbesserung kriti-

scher Infrastrukturen gelangen. Insbesondere Schwachpunkte an der Schnittstelle zwischen den organisationalen Abläufen und dem Umgang mit IT und den IT-Systemen selbst sind Einfallsorte für doloses und kriminelles Verhalten von Kriminellen und Spionageagenturen. So können etwa gezielt Sicherheitslücken oder zu schwache Passwörter in Meta-Systemen ausgenutzt werden, um etwa über den Mobilfunkanschluss oder die Mitgliedschaft in einem Bonusprogramm an Unternehmenszugänge zu gelangen. Daraus wird ersichtlich, dass ein hervorragend gesichertes internes IT-System durch unachtsamen Umgang damit kompromittiert werden kann und dass umgekehrt ein unzureichend gesichertes IT-System keine geeignete Unterstützung für ansonsten sehr gute Organisationsabläufe sein kann.

Daher gehört die Beherrschung der eigenen, aber darüber hinaus auch der mit den eigenen Systemen verbundenen Systeme zu den größten technischen und organisatorischen Herausforderungen. Benötigt werden Systeme, die anpassungsfähig und zugleich resilient und robust sind. Aus diesem Grund wird in diesem Abschnitt auf die Bedeutung der organisationalen Kultur in Behörden und deren Rolle für den sicheren und robusten Umgang mit kritischen IT-Systemen eingegangen. Hierzu gehört ein systemisches Denken, Planen und Anwenden von in Verwaltungen eingesetzten, vernetzten IT-Systemen, was ein erhöhtes Maß an Bewusstsein und Achtsamkeit für kontextspezifische Gegebenheiten erfordert. Ein zentraler Erfolgsfaktor hierfür ist die sog. organisationale Achtsamkeit (engl. „Mindfulness“), welche kognitive Fähigkeiten und eine Kultur des mitdenkenden Handelns auf Unternehmensebene beschreibt. Organisationen, die durch organisationale Achtsamkeit gekennzeichnet sind, sind besser in der Lage, mit unvorhergesehenen Ereignissen umzugehen, verfügen über IT-Systeme, die sie besser in ihren Aufgaben unterstützen und die somit Unsicherheiten, die aus dem Umgang mit kritischen IT-Infrastrukturen erwachsen, begegnen können.

Das Konzept der organisationalen Achtsamkeit entstammt ursprünglich der Organisationstheorie und expliziert das organisationale Metawissen über die inhärente Präsenz von begrenzter Rationalität und Fehlerhaftigkeit. Insbesondere drückt sich organisationale Achtsamkeit in einer hohen Resistenz gegenüber Vereinfachungen („Reluctance to Simplify“), einer erhöhten operativen Sensitivität („Operational Sensitivity“), einem hohen Fehlerbewusstsein („Preoccupation with Failure“), einer starken Mobilisierungs- und Stabilisierungskraft („Commitment to Resilience“) sowie einer erhöhten Achtung der Fachkompetenz („Deference to Expertise“) aus. Gemäß der Theorie zu dynamischen Fähigkeiten in Organisationen umfasst das Konzept der organisationalen Achtsamkeit grundlegende kognitive Mechanismen, die in Kombination mit geeigneten IT-Systemen vor allem den Aufbau von erweiterten „Sensing“-Fähigkeiten einer Organisation unterstützen. Diese Fähigkeiten wiederum ermöglichen die schnellere Beurteilung von Auswirkungen, die sich durch Veränderungen oder Störungen in IT-Systemen ergeben und verringern somit irrationale Entscheidungen und vorschnelle mimetische Verhaltensweisen und deren negative Konsequenzen.

2. Herausforderungen in der IT-Integration aus organisationaler Sicht

Die effektive und effiziente Integration von IT-Systemen in bestehende Systeme und Verfahrensabläufe stellt eine der größten Herausforderungen für das Verwaltungsmanagement dar. Planungsfehler wie beim Neubau der Zentrale des Bundesnachrichtendienstes oder mangelnde Berücksichtigung von unerwünschten Interaktionseffekten mit bestehenden Systemen führen zu erheblichen Mehraufwendungen und suboptimalen Systemen aufgrund notwendiger Nachbesserungen, etwa wenn sich die eingeführte Verschlüsselungsinfrastruktur wegen Sicherheitslücken als ungeeignet herausstellt.

Die bestehende Forschung im Kontext von IT-Systemassimilation konzentriert sich bisher primär auf die technologischen Vorteile und Herausforderungen, wie z. B. bestehenden Protokoll-Overhead, fehlende Aushandlungsmechanismen für Service Level Agreements, unflexible Abrechnungsstrukturen sowie bestehende Sicherheitsmängel. Neben diesen technischen Herausforderungen scheitern Verwaltungen und Unternehmen bei der Einführung neuer IT-Systeme aber insbesondere an organisationalen Einflussfaktoren wie z. B. einem zu wenig berücksichtigten Interaktionsverhalten mit Alt-Systemen, der Nicht-Nutzung der neuen Systeme durch den eigentlichen Anwender oder der Umwidmung und Nutzung der IT-Systeme in einer nicht beabsichtigten Art und Weise. Werden in einem derartigen Umfeld weitere Systeme integriert, so erschwert dies die Vorhersagbarkeit möglicherweise eintretender systembedingter Effekte, verringert unter Umständen die Leistungsfähigkeit bestehender Systeme oder schafft Systemrisiken für Altsysteme, die bei der Implementierung des neuen IT-Systems nicht in Erwägung gezogen wurden. Letztlich schlägt sich eine derartige ungewollte Verschlechterung des Gesamtsystems auch auf die Prozess- und Verfahrensqualität nieder.

In den folgenden Abschnitten werden Ergebnisse aus einer aktuellen Studie aufgezeigt, die in einem Landesministerium durchgeführt wurde. Dabei wurde untersucht, wie unterschiedlich stark ausgeprägte Formen von Achtsamkeit die Effektivität und Nutzung einer für das Ministerium kritischen IT-Infrastruktur beeinflussen.

3. Verteiltes Arbeiten und „Workplace-as-a-Service“ als kritische Infrastruktur in Verwaltungen

Was zunächst als virtualisierte Rechenleistung und Speicherkapazität von Unternehmen wie Google, Amazon und IBM angeboten wurde, um deren ungenutzte Kapazitäten über das Internet zu vertreiben, hat sich mittlerweile als Cloud Computing fest etabliert und ebenfalls im öffentlichen Sektor Einzug gehalten[120]. Auch wenn aus Sicherheitsgründen nicht alle cloud-basierten Dienstleistungen von öf-

[120] Vgl. zum Cloud Computing in der öffentlichen Verwaltung auch bereits die Nachweise in Fn. 80.

fentlich zugänglichen Cloud-Anbietern genutzt werden, so gewinnen doch gerade intern betriebene Cloud-Anwendungen zunehmend an Bedeutung, um die Effektivität der IT sowie die Effizienz der unterstützen Verfahren weiter zu steigern. Gleichzeitig erfüllt Cloud Computing Anforderungen der öffentlichen Verwaltung bezüglich Flexibilität, Skalierbarkeit und Zuverlässigkeit von IT, insbesondere im Bereich der Unterstützung der Angestellten an deren Arbeitsplatz. So lassen sich mittels cloud-basierten Arbeitsplatzumgebungen Arbeiten nicht mehr nur noch am Arbeitsplatz-PC verrichten, sondern auch von anderen Arbeitsplätzen innerhalb der Verwaltung oder aber von anderen Endgeräten, etwa dem heimischen PC oder aber über Tablets, von unterwegs. Diese zentral vorgehaltene Arbeitsplatzumgebung oder „Workplace-as-a-Service“ (kurz: WaaS) sichert somit nicht nur eine einheitliche Anwendungsumgebung für die Nutzer, unabhängig vom Endgerät, sondern ermöglicht darüber hinaus auch eine Standardisierung der Anwendungsumgebung über verteilte Standorte, was zusätzlich zur Stabilität und Kosteneffizienz beiträgt.

Die Daten und die Anwendung einer solchen WaaS-Umgebung werden konsolidiert und zentral auf virtualisierten Servern vorgehalten, was zu einer erhöhten Datenkonsistenz im Vergleich zur Datenhaltung auf herkömmlichen dezentralen Desktops führt. WaaS kombiniert somit Vorteile virtualisierter Desktops mit Cloud-basierten Lösungen wie „Infrastructure-as-a-Service“, also virtualisierte Server und Datenhaltung, sowie „Software-as-a-Service“, wie etwa das Vorhalten von Betriebssystemen und Anwendungen, die auf das Endgerät über das Internet übertragen werden.

Zusätzlich kann WaaS Sicherheitsrisiken reduzieren helfen, die bei Verlust sensibler Daten oder im Falle von Diebstahl etwa von Laptops entstehen können, da die Daten zentral gespeichert werden und nicht auf dem Gerät. Derart mit den Vorteilen des Cloud Computing kombiniert bietet WaaS technischen und wirtschaftlichen Nutzen.

4. Interaktion von achtsamem Handeln und „Workplace-as-a-Service“

Zur Ermittlung der Nutzenpotenziale von WaaS in der öffentlichen Verwaltung und der Rolle der organisationalen Kultur im Umgang mit diesem Dienst wurde eine fragebogenbasierte Umfrage unter Nutzern von WaaS in einem deutschen Justizministerium durchgeführt. Anhand von 257 ausgefüllten Fragebögen konnte ein Einfluss der Eigenschaften von WaaS, wie bspw. flexible Zugriffsmöglichkeiten, die Korrektheit benötigter Informationen sowie die Flexibilität und Verlässlichkeit der eingesetzten Systeme, auf die Produktivität und Kreativität der Mitarbeiter bei der Erledigung ihrer täglichen Aufgaben nachgewiesen werden. Zur genaueren Analyse dieses Zusammenhangs wurde die Stichprobe abhängig vom individuellen Maß organisationaler Achtsamkeit in zwei Gruppen geteilt, um den Einfluss von Technologien wie WaaS auf die Unterstützung der Verfahren und Aufgaben in der öffentli-

chen Verwaltung zu untersuchen sowie um den Einfluss der Achtsamkeit der Verwaltungsmitarbeiter besser zu verstehen.

Das der Studie zugrunde liegende Forschungsmodell identifiziert Erfolgsfaktoren hinsichtlich der Effektivität von Investitionen in Informationssysteme und des Einsatzes derselben. Das Modell umfasst sechs in Abhängigkeit zueinander stehende Dimensionen: Systemqualität, Informationsqualität, Servicequalität, Nutzung, Nutzerzufriedenheit und von Nutzern wahrgenommene Vorteile von WaaS. Bspw. beschreibt das Modell den Einfluss der drei Dimensionen Informationsqualität, Systemqualität und Servicequalität auf die Nutzung und die Nutzerzufriedenheit. Letztere beeinflussen sich wechselseitig und bedingen wiederum die Wahrnehmung hinsichtlich der Vorteile des Systems.

Zur Untersuchung von Achtsamkeit und deren Bedeutung im Umgang mit kritischen IT-Infrastrukturen in der Verwaltung wurden im April 2013 insgesamt 850 Mitarbeiter eines deutschen Justizministeriums zu ihrem Nutzungsverhalten hinsichtlich des im Einsatz befindlichen WaaS-Systems befragt. Insgesamt wurde mit 257 ausgefüllten Fragebögen eine Rücklaufquote von 30,24 % erreicht. Mit dem WaaS-System können die Mitarbeiter (z. B. bei Nutzung aus dem Home Office) auf ihr individuelles Nutzerprofil, die Informationen und Daten sowie Programme unabhängig vom genutzten Endgerät zugreifen. Dies ermöglicht ihnen eine größere Flexibilität verglichen mit klassischen Desktopsystemen am Arbeitsplatz, setzt aber auch einen verantwortungsbewussteren Umgang damit voraus. Die Datenverarbeitung selbst erfolgt zentralisiert auf den cloud-basierten Servern, auf die mittels Thin-Clients zugegriffen wird. Wie bereits erwähnt, ist dies eines der zentralen Gründe, die zu einer sichereren und konsistenteren Datenhaltung bei Nutzung von WaaS beitragen.

5. Verbesserte und robustere Verfahren durch „Workplace-as-a-Service“

Zunächst war die erste Forschungsfrage nach der Wirkung der verschiedenen WaaS-Charakteristika auf den Zusammenhang von Nutzung und Nutzungszufriedenheit sowie der wahrgenommenen Vorteile des Informationssystems zu beantworten. Hier konnte gezeigt werden, dass die Systemqualität in Form von Zugriffsmöglichkeiten und Geschwindigkeit sowie Flexibilität und Verlässlichkeit des Systems einen signifikanten Einfluss auf die Nutzung und Nutzerzufriedenheit haben. Besonders der zeit- und ortsunabhängige Zugriff auf Programme und Daten sowie die flexible Anpassung von WaaS an verschiedene Situationen fördern die durch den Nutzer wahrgenommenen Vorteile von WaaS. Darüber hinaus besitzt die Informationsqualität, im Sinne von Genauigkeit und Aktualität der Daten, einen positiven Einfluss auf die Nutzerzufriedenheit und die wahrgenommenen Vorteile. Im Gegensatz dazu konnte kein Einfluss der Servicequalität auf die Nutzerzufriedenheit festgestellt werden. Dies kann mit der Analyseebene begründet werden, die in dieser Studie nicht auf dem WaaS-Dienstleister, sondern auf der Anwendbarkeit von WaaS bei täglichen Aufgaben lag.

Bezüglich der Unterschiede der stark und schwach organisational achtsamen Mitarbeiter zeigten sich überraschende Ergebnisse. Zunächst konnte gezeigt werden, dass das WaaS-System signifikant größere Vorteile für die weniger achtsamen Mitarbeiter bietet im Vergleich zu den stärker achtsamen. Dies kann allerdings auch mit der Annahme erklärt werden, dass stark achtsame Mitarbeiter bereits eine größere Leistung und Innovation zeigen als weniger achtsame Mitarbeiter. Es zeigt aber auch, dass WaaS kritische Verfahren verbessern helfen kann, indem es insbesondere Verwaltungsangestellte unterstützt, die sich durch eine geringere individuelle Achtsamkeit auszeichnen. Darüber hinaus war ein größerer Einfluss der Nutzung auf die wahrgenommenen Systemvorteile und eine größere Nutzungszufriedenheit bei den weniger achtsamen Mitarbeitern feststellbar. Diese geringere Zufriedenheit kann mit der stärkeren Tendenz zur Beschäftigung mit Fehlern und der Abneigung von Vereinfachungen stark achtsamer Menschen erklärt werden. Unerwartet war hingegen der stärkere Einfluss von Nutzerzufriedenheit auf die wahrgenommenen Systemvorteile in der Gruppe der achtsameren Mitarbeiter. Eine mögliche Erklärung hierfür wäre bspw. die übergeordnete Bedeutung der Nutzungszufriedenheit in dieser Gruppe. Dementsprechend konnte auch die zweite Forschungsfrage hinsichtlich der unterschiedlichen Wahrnehmung der Systemvorteile von WaaS als kritische IT-Infrastruktur in Verwaltungen von Mitarbeitern mit erhöhter und geringerer organisationaler Achtsamkeit beantwortet werden.

Die Ergebnisse der Studie belegen, dass zum Schutz kritischer Systeme die Faktoren Mensch und Organisation von entscheidender Bedeutung sind. Individuelle und organisationale Achtsamkeit sind notwendig, um kritische Systeme in der Verwaltung sicher einsetzen zu können. Aber auch die Systeme selbst, wie am Beispiel WaaS gezeigt, tragen zur verantwortungsvollen und sicheren Nutzung bei. Wie gezeigt werden konnte, unterstützen Systeme, die als nützlich angesehen werden und positiv auf die Erfüllung der Aufgaben wirken, insbesondere weniger achtsame Mitarbeiter, was gerade bei dieser Gruppe zu einer deutlichen Verbesserung im sicheren Umgang mit kritischen Infrastrukturen führt.

H. Ausblick

Die Analyse konnte einerseits die Einordnung bestimmter IT-Systeme und Komponenten, auf denen das Internet basiert, als kritische Infrastrukturen belegen, andererseits denkbare Handlungsfelder skizzieren. Diese lassen sich zwar dem Grunde nach in technische, organisationale und rechtliche Maßnahmen unterteilen, die Komplexität der Bedrohung und die Vernetzung der Systeme lassen aber gleichwohl nur eine Kombination verschiedener Elemente als zielführende Reaktion erscheinen. Insofern muss eine interdisziplinäre Anschlussforschung diese Besonderheit berücksichtigen. Folgende Forschungsfragen lassen sich exemplarisch benennen:

- Die effektive und effiziente Integration (Assimilierung) von IT-Systemen in bestehende Systeme und Prozessabläufe stellt eine der größten Herausforderungen für das Management in Behörden und Unternehmen dar. Fehler oder Ineffizienzen oder die mangelnde Berücksichtigung von unerwünschten Interaktionseffekten mit bestehenden Systemen im IT-Assimilierungsprozess führen hierbei zu erheblichen Problemen und finanziellen Verlusten. Die bestehende Forschung im Kontext von IT-Assimilierung konzentriert sich bisher aber primär auf die technologischen Vorteile und Herausforderungen. Neben den technischen Herausforderungen scheitern Firmen bei der IT-Assimilierung aber insbesondere an organisationalen Einflussfaktoren, wie z. B. einem zu wenig berücksichtigten Interaktionsverhalten mit Altsystemen. Die Assimilierung von weiteren Systemen erschwert zunehmend die Vorhersagbarkeit möglicherweise eintretender systembedingter Effekte, verringert unter Umständen die Leistungsfähigkeit bestehender Systeme oder schafft Systemrisiken für Altsysteme, die bei der Implementierung des neuen IT-Systems nicht in Erwägung gezogen wurden. Letztlich schlägt sich eine derartige Verschlechterung des Gesamtsystems, welches als das „System der Systeme“ definiert werden kann, auch auf die zu unterstützenden Prozesse und Verfahren nieder.

  Daher wäre der vorherrschende technozentrische Fokus auf die Assimilierung von einzelnen IT-Systemen um die Betrachtung von zentralen organisationalen und situativen Determinanten zu erweitern, die den resultierenden Erfolg von Gesamtsystemen bestimmen. Hinzu tritt die Identifikation und Bewertung flankierender rechtlicher Mechanismen, um individuelle und organisationale Achtsamkeit im Umgang mit kritischen IT-Systemen in der öffentlichen Verwaltung zu etablieren und verbindlich auszugestalten. Es sollten daher sowohl Systemplanungsansätze als auch Organisationskulturen untersucht und evtl. bereits zur Anwendung kommende rechtliche Mechanismen

(Dienstanweisungen o. ä.) identifiziert werden, die Einfluss nehmen auf die Stabilität, Nutzung und Effektivität kritischer Infrastrukturen im öffentlichen Sektor. Ziel eines Forschungsvorhabens wäre es, eine integrative Perspektive auf IT-Systemassimilierung im öffentlichen Sektor zu entwickeln. Hierzu ließen sich in einer quantitativen Feldstudie sowohl die im Einsatz befindlichen Systemplanungsansätze ermitteln als auch der Grad der organisationalen Achtsamkeit untersuchen, die erheblichen Einfluss sowohl auf die Systemplanungsfähigkeiten als auch die Widerstandsfähigkeit des gesamten IT-Systems haben dürfte.

- Im Bereich Smart Cities wird von der intelligenten Vernetzung komplexer, auch kritischer Systeme die Steigerung der Effizienz und Lebensqualität erwartet. Die Steigerung der Effizienz erfolgt durch Wiederverwendung von Standard-Systemkomponenten und Einbeziehung umfangreicher Daten, auch aus traditionell zunächst fachfremden Bereichen. Gleichzeitig wird ein qualitativer Gewinn erwartet, bspw. als Beitrag zur Lösung von gesellschaftlichen Herausforderungen (Energiewende, Alterung der Gesellschaft usw.). Der Begriff intelligente Vernetzung beschreibt dabei die Verknüpfung einer Infrastruktur mit Informations- und Kommunikationstechnologie, sodass eine Regelung oder Koordination der gesamten Infrastruktur oder ihrer Teile mittels IuK-Technologie möglich ist. Intelligente Netze bezeichnen in diesem Zusammenhang neuartige, vernetzte Anwendungen und Verknüpfungen von Daten (vergleichbar mit sozialen Netzen) und nicht direkt die unterliegende Übertragungstechnik (wie im Begriff Kommunikationsnetze).

  Die Anwendungsbereiche dieser intelligenten Vernetzung sind vielseitig – im Mittelpunkt der gegenwärtigen Diskussion stehen die Bereiche Energie, Verkehr, Gesundheit, Bildung und öffentliche Verwaltung. Zu diesen ganz unterschiedlichen Anwendungsbereichen gehören u. a. auch kritische Infrastrukturen.

  Die verschiedenen Anwendungsbereiche verfügen jeweils über ein gewachsenes Regime von Vorgaben und Best Practices, vor allem auch im Kontext der IT-Sicherheit. Insbesondere im Bereich kritischer Infrastrukturen kommt die gesetzliche Regulierung hinzu. Grundsätzlich kann zwischen drei Graden von Vorgaben oder Regulierung unterschieden werden:

- nicht oder wenig regulierte Anwendungen, bspw. klassische Bereiche der Softwareindustrie,
- regulierte Anwendungen im Bereich Informations- und Kommunikationstechnologie,
- regulierte Anwendungen klassischer Infrastrukturen bzw. nichttechnische Vorgaben.

Ziel eines Forschungsprojekts könnte die Entwicklung einer Methodik zur Identifikation einer realistischen Auswahl von Komponenten und Schnittstellen sein, um die Zusammenarbeit zwischen verschiedenen Anwendungsbereichen intelligenter Vernetzung zu ermöglichen. Vor allem das Aufeinandertreffen von regulierten (bspw. im Kontext kritischer Infrastrukturen) und nicht-regulierter Bereiche (bspw. der eingesetzten Software) stellt sich dabei als besondere Herausforderung dar. Basis wäre die Darstellung eines exemplarischen Modells zur Betrachtung der Kombination von Anwendungen und teilweise gemeinsam genutzten Komponenten bzw. gemeinsamen Schnittstellen: Beispielhaft könnten Anwendungen im Zusammenhang mit kritischen Infrastrukturen sein, die hohen technischen und regulatorischen Anforderungen genügen müssen.

Im Verlag des Lorenz-von-Stein-Instituts erscheinen folgende Schriftenreihen

A r b e i t s p a p i e r e

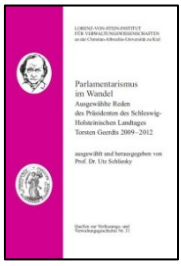
- **AP 102: Brüning u. a.,** Die Rolle der Kommunen bei der Vergabe von Konzessionen nach § 46 EnWG
- **AP 100: Werner,** Vermögensabgabe - eine empirische Untersuchung
- **AP 99: Brüning (Hrsg.),** Prüfungskompetenzen der Rechnungshöfe bei ausgegliederter Aufgabenwahrnehmung

L a n d e s r e c h t S c h l e s w i g - H o l s t e i n

- **LSH 1.5: Hoefer (Hrsg.),** Gesetze des Landes Schleswig-Holstein (Textsammlung), 5. Aufl. 2014
- **LSH 2: Caspar/Ewer/Nolte/Waack (Hrsg.),** Verfassung des Landes Schleswig-Holstein (Kommentar)

M o d e r n i s i e r u n g v o n S t a a t u n d V e r w a l t u n g

- **MSV 18: Bosesky u. a.,** Datenhoheit in der Cloud
- **MSV 17: Schliesky u. a.,** Arbeitsteilung 2.0 - Kollaboratives Arbeiten der deutschen Verwaltung
- **MSV 16: Luch/Schulz,** Das Recht auf Internet als Grundlage der Online-Grundrechte



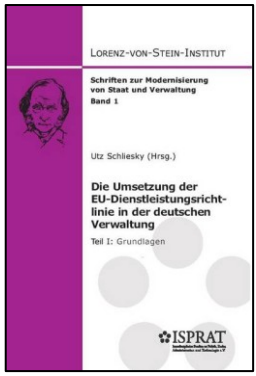
Q u e l l e n z u r V e r f a s s u n g s - u n d V e r w a l t u n g s g e s c h i c h t e

- **VG 34: Welti,** Lorenz von Stein und das Recht auf eine gute Sozialverwaltung
- **VG 33: Hering**, Lorenz von Stein und Schleswig-Holstein im Europa der Revolutionen 1848/49
- **VG 32: Taschke**, Dokumente aus dem Leben Lorenz von Steins

S c h r i f t e n r e i h e

- **SR 24: Blasius,** Lorenz von Stein - Deutsche Gelehrtenpolitik in der Habsburger Monarchie
- **SR 23: Nolte,** Staatliche Verantwortung im Bereich Sport
- **SR 22: Behrndt,** Neues Verwaltungsmanagement und kommunales Verfassungsrecht

Lorenz-von-Stein-Institut
für Verwaltungswissenschaften



Sonderpreis:

Alle drei Bände für 149,90 € (statt 167,00 €)

Die Umsetzung der EU-Dienstleistungsrichtlinie in der deutschen Verwaltung

Prof. Dr. Utz Schliesky (Hrsg.)

Teil I – Grundlagen
2008, 236 S., ISBN: 978-3-936773-34-7, 49,- €

Aus dem Inhalt:

Das Ende der deutschen Verwaltung? (Schliesky)

Der personelle Anwendungsbereich der EU-Dienstleistungsrichtlinie (Luch/Schulz)

Der sachliche Anwendungsbereich der EU-Dienstleistungsrichtlinie (Luch/Schulz)

Einheitlicher Ansprechpartner: Umsetzungsmodell zum Ablauf des Verwaltungsverfahrens (Neidert)

und zahlreiche weitere Beiträge

Teil II – Verfahren, Prozesse, IT-Umsetzung
2009, 324 S., ISBN: 978-3-936773-48-4, 59,- €

Aus dem Inhalt:

Auswirkungen der DLR auf das Gewerberecht (Kluth)

Grundsatz der Unternehmerfreundlichkeit im Verwaltungsverfahren? (Korte)

Zwang zur Netzwerkverwaltung am Beispiel der DLR (Schliesky)

Änderungsbedarf im Verwaltungsverfahrensrecht aufgrund der DLR (Ramsauer)

und zahlreiche weitere Beiträge

Teil III – Information, Wissen und Verantwortung
2010, 352 S., ISBN: 978-3-936773-57-6, 59,- €

Aus dem Inhalt:

Die Umsetzung der EU-Dienstleistungsrichtlinie als (gescheiterter) Innovationsprozess? (Schliesky)

Datenschutz im Rahmen der elektronischen Verfahrensabwicklung (Neidert)

Reichweite der Informationsverpflichtungen staatlicher Stellen aus der EU-Dienstleistungsrichtlinie (Schulz)

Verantwortlichkeiten in geteilten Wissensmanagement-Systemen (Altmann)

und zahlreiche weitere Beiträge zur Umsetzung der Richtlinie in Deutschland

Lorenz-von-Stein-Institut
für Verwaltungswissenschaften

In den „Schriften zur Modernisierung von Staat und Verwaltung“ sind zuletzt folgende Werke erschienen:

MSV 18	**Datenhoheit in der Cloud** Pino Bosesky u. a. Kiel, 2013, 110 S. ISBN: 978-3-936773-84-2	39,- €
MSV 17	**Arbeitsteilung 2.0 – Kollaboratives Arbeiten der deutschen Verwaltung** Utz Schliesky u. a. Kiel, 2013, 112 S. ISBN: 978-3-936773-81-1	29,- €
MSV 16	**Das Recht auf Internet als Grundlage der Online-Grundrechte** Anika D. Luch / Sönke E. Schulz Kiel, 2013, 94 S. ISBN: 978-3-936773-80-4	29,- €
MSV 15	**Shared Service Center als innovative Organisationsform** Maximilian Tallich Kiel, 2012, 302 S. ISBN: 978-3-936773-78-1	39,- €
MSV 14	**Der *E-POSTBRIEF* in der Kommunalverwaltung – Einsatzoptionen für kommunale Fachverfahren** Franziska Brackmann/Sönke E. Schulz/Jakob Tischer/ Thomas Warnecke Kiel, 2012, 160 S. ISBN: 978-3-936773-74-3	29,- €
MSV 13	**Die Gewährleistung der Vertraulichkeit und Integrität elektronischer Daten- und Dokumentensafes** Christian Hoffmann Kiel, 2012, 298 S. ISBN: 978-3-936773-72-9	39,- €

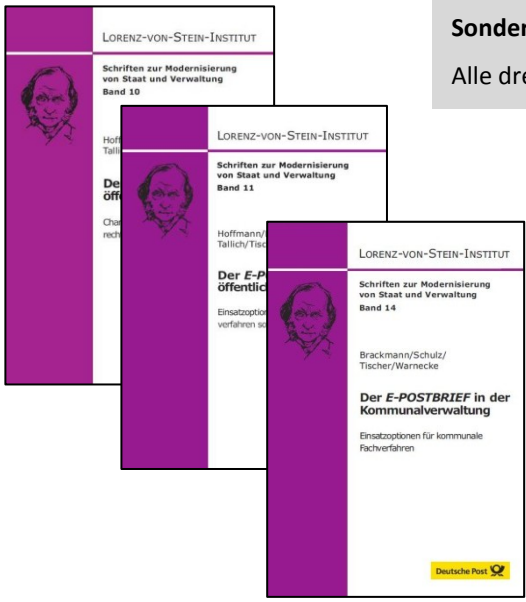
MSV 12	**Transparenz, Partizipation, Kollaboration – Web 2.0 für die öffentliche Verwaltung** Utz Schliesky/Sönke E. Schulz (Hrsg.) Kiel, 2012, 235 S. ISBN: 978-3-936-773-71-2	39,- €
MSV 11	**Der *E-POSTBRIEF* in der öffentlichen Verwaltung – Einsatzoptionen im Sozial- und Steuerverfahren sowie für Berufsgeheimnisträger** Christian Hoffmann/Anika D. Luch/Sönke E. Schulz/ Maximilian Tallich/Jakob Tischer Kiel, 2011, 150 S. ISBN: 978-3-936773-69-9	29,- €
MSV 10	**Der *E-POSTBRIEF* in der öffentlichen Verwaltung – Chancen, Einsatzoptionen und rechtliche Handlungsspielräume** Christian Hoffmann/Anika D. Luch/Sönke E. Schulz/ Maximilian Tallich/Jakob Tischer/Thomas Warnecke Kiel, 2011, 156 S. ISBN: 978-3-936773-65-1	29,- €
MSV 9	**Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** Lutz Drallé Kiel, 2010, 175 S. ISBN: 978-3-936773-60-6	34,- €
MSV 8	**Staatliches Innovationsmanagement** Utz Schliesky (Hrsg.) Kiel, 2010, 394 S. ISBN: 978-3-936773-61-3	74,- €

Online-Shop:
www.lorenz-von-stein-institut.de

Eine vollständige Auflistung aller Publikationen, die im Eigenverlag des Lorenz-von-Stein-Instituts veröffentlicht wurden, sowie weitergehende Informationen finden Sie im Internet unter:
http://www.lvstein.uni-kiel.de

Die Publikationen können unter folgender Adresse bestellt werden:
Lorenz-von-Stein-Institut für Verwaltungswissenschaften
an der Christian-Albrechts-Universität zu Kiel
Olshausenstraße 40, 24098 Kiel
oder per Telefon: (0431) 880-4542,
per Fax: (0431) 880-7383
bzw. im Internet unter: http://www.lvstein.uni-kiel.de

Lorenz-von-Stein-Institut
für Verwaltungswissenschaften



Sonderpreis:

Alle drei Bände für 69,90 € (statt 87,00 €)

Der *E-POSTBRIEF* in der öffentlichen Verwaltung

Teil I: Chancen, Einsatzoptionen und rechtliche Handlungsspielräume

Christian Hoffmann/Anika D. Luch/Sönke E. Schulz/
Maximilian Tallich/Jakob Tischer/Thomas Warnecke
Kiel, 2011, 156 S.
ISBN: 978-3-936773-65-1

Teil II: Einsatzoptionen im Sozial- und Steuerverfahren sowie für Berufsgeheimnisträger

Christian Hoffmann/Anika D. Luch/Sönke E. Schulz/
Maximilian Tallich/Jakob Tischer
Kiel, 2011, 150 S.
ISBN: 978-3-936773-69-9

Teil III: Einsatzoptionen für kommunale Fachverfahren

Franziska Brackmann/Sönke E. Schulz/
Jakob Tischer/Thomas Warnecke
Kiel, 2012, 160 S.
ISBN: 978-3-936773-74-3