Eckpunktepapier für ein Identitätensicherheitsgesetz im Internet der Dinge – Version 2

Inhaltsverzeichnis

I. Executive Summary

Das Internet der Dinge („IoT"), also die allumfassende Vernetzung intelligenter Geräte miteinander über das Internet, ist auf dem Vormarsch und wird bereits in den kommenden fünf Jahren Realität werden. Die entscheidende Veränderung, die das IoT mit sich bringen wird, ist seine Ubiquität: Vernetzte Geräte sind überall. Wie jeder technologische Fortschritt bietet diese Entwicklung gesellschaftliche und wirtschaftliche Chancen, sie bringt aber auch Risiken mit sich:

- Im IoT stellt derzeit jedes vernetzte Gerät einen potentiellen Angriffspunkt für Hacker dar. Fast täglich ist in den Nachrichten von Angriffen auf vernetzte Geräte zu lesen, sei es die Übernahme der Steuerung eines Autos oder der Zugriff auf die Funktionen eines Narkosegerätes.[1] Die Einfallstore für unberechtigte Zugriffe von Dritten sind in den allermeisten Fällen Schwachstellen der Software.
- Kein Nutzer von vernetzten Geräten – Unternehmen und Verbraucher – kann heute darauf vertrauen, dass die Geräte und die Datenflüsse der Geräte tatsächlich nur die Funktionen und Datenflüsse aufweisen und ausführen, die die dafür berechtigten Personen bzw. Stellen festgelegt haben. Dem entsprechend sind die tatsächlich ausgeführten Funktionen und stattfindenden Datenflüsse von Geräten im IoT heute auch nicht sicher nachvollziehbar.

Um den Schutz der Daten und die Sicherheit vernetzter Geräte in Zukunft zu garantieren und damit das Vertrauen in das vernetzte Alltags- und auch Wirtschaftsleben zu stärken, bedarf es gesetzlicher Vorsorgemaßnahmen, die risikominimierend, technikneutral und innovationsoffen sind. Diese sollten sich **sektorenübergreifend** auf die **Komponenten** der vernetzten Geräte beziehen, um eine datensichere und datenschutzfreundliche, auf gemeinsamen Standards basierende Kommunikation der Geräte zu ermöglichen. Über eine Zertifizierung ist sicherzustellen, dass die in der EU – zum Schutz der

Wirtschaft wenigstens jedoch in Deutschland – in Verkehr gebrachten vernetzten Geräte diese Vorgaben erfüllen. Kernbestandteil solcher gesetzlicher Vorgaben ist das Verbot für Gerätehersteller, vernetzbare Geräte zu vertreiben, die bestimmte **Mindestanforderungen** nicht erfüllen:

- Die Kommunikation mit anderen IoT-Geräten und die Datenverarbeitung erfolgt standardisiert stets über einen verschlüsselten, integritätsgesicherten Kanal.
- Auf Hardwareebene ist unveränderlich festgelegt, dass nur ein oder mehrere definierte Berechtigte Zugriff auf die Hardware nehmen dürfen.
- Eine gegenseitige Authentisierung der Kommunikationspartner ist erforderlich.
- Welche Funktionen das Gerät besitzt, welche Datenverarbeitungen erfolgen, an welche Geräte Daten übermittelt werden, wird unveränderlich festgelegt.
- Nur die Berechtigten dürfen diese Einstellungen zur Kommunikation und Funktionalität ändern.
- Es sind unveränderliche Zweckfelder vorzusehen, über die allein die Berechtigten fakultativ bestimmen können, zu welchen Zwecken bestimmte Daten aus dem vernetzten Gerät von autorisierten Dritten verwendet werden dürfen.

Dabei sollen vernetzte Geräte stets den geltenden **Stand der Technik** einhalten.

Legislative Regelungen bieten die Gewähr dafür, dass diese Vorgaben beachtet werden. Ansätze einer ausschließlichen Selbstregulierung oder die Schaffung nur verbandsinterner Standards können dieser wichtigen technologischen Entwicklung nicht den dringend erforderlichen Regulierungsrahmen geben. Das Verbot, technische Geräte in Verkehr zu bringen, die gewisse Mindeststandards nicht erfüllen oder das Gebot, eigene IT-Infrastrukturen gegen Angriffe zu schützen, ist dem europäischen und deutschen Recht bereits bekannt. Jedoch zielen die geltenden Regelungen (z.B. IT-Sicherheitsgesetz; Energiewirtschaftsgesetz) auf bestimmte Wirtschaftssektoren und besondere Anwendungsbereiche ab. Mit dem explosionsartigen Anstieg vernetzter Geräte bleiben die Risiken jedoch nicht auf diese einzelnen Bereiche beschränkt, sondern erwachsen aus der Existenz der Geräte und deren Vernetzung an sich. Die Mindestvorgaben eines **Identitätensicherheitsgesetzes** gelten daher unabhängig vom betroffenen Lebens- oder Wirtschaftsbereich.

II. Einleitung

Die Digitale Agenda der Bundesregierung hat den Schutz der Nutzer, Sicherheit und Systembeherrschbarkeit in der vernetzten Welt des Internets der Dinge („Internet of Things“) als zentrale Herausforderungen benannt. Nach aktuellen Schätzungen werden bis zum Jahr 2020 mindestens 50 Milliarden Identitäten (d.h. beteiligte Menschen und vernetzte Geräte) mit einander vernetzt sein. Die Sicherheit der Informations- und Kommunikationstechnologie („IKT“) und der Datenschutz sind Voraussetzungen für das Vertrauen in digitale Dienste und neue Geschäftsmodelle. Es muss grundsätzlich sichere vernetzte Geräte geben, um Identitäten im Netz besser zu schützen und sicher kommunizieren zu können.

Effektive, bereits auf Hardwareebene implementierte Lösungen können die Anwender (Bürgerinnen und Bürger ebenso wie Unternehmen) als handelnde **Identitäten** in den Mittelpunkt stellen,[2] um den Rechtsrahmen sowie bewährte Regeln aus der „analogen“ Welt auf die digitale, hochvernetzte Welt zu übertragen. Hierzu müssen sich Identitäten gegenseitig eindeutig identifizieren und diese zugleich sicher authentifiziert werden können. Die Daten selbst und die Kommunikation von Identitäten im Netz sowie die Funktionen der Geräte und zu welchen Zwecken diese ausgeführt werden, sind so zu schützen, dass Menschen und Unternehmen die Kontrolle behalten und Transparenz hinsichtlich der Datennutzung und der Sicherheit vernetzter Geräte besteht.

Die aktuelle Gesetzeslage in Deutschland und Europa gibt sowohl bei Fragen des Datenschutzes als auch der IT-Sicherheit für die IoT-Infrastruktur nur partielle, auf bestimmte Anwendungsfelder und Branchen beschränkte Antworten. Erforderlich ist jedoch ein sektorenübergreifender, legislatorischer

Ansatz, der alle Identitäten umfassend schützt und verwaltet.
Ein bedeutendes Ziel der Digitalen Agenda der Bundesregierung, nämlich „*bei der digitalen Transformation durch **gesetzliche Anforderungen** oder mit **allgemeinverbindlichen Standards** für ein hohes Niveau an Sicherheit sorgen*“ und dazu „*Maßnahmen zur Sicherung der Vertrauenswürdigkeit der digitalen Infrastrukturen*“ zu ergreifen, kann erreicht werden, wenn die EU oder wenigstens Deutschland mit einem **Identitätensicherheitsgesetz im Internet der Dinge** vorangeht, das die Zulassungs- und Verkehrsfähigkeit von IoT-Geräten regelt und dabei folgende Prinzipien eines effektiven Sicherheitskonzepts umsetzt:

- **Security by Design** – Jede mit dem Internet der Dinge verbundene Identität muss technisch geschützt werden. Das heißt, jedes mit dem Netz verbundene Gerät ist mit einem kryptografisch gesicherten Hardwarezugang auszustatten.
    - Alle mit dem Internet der Dinge verbundenen Identitäten sollen nur diejenigen Daten kommunizieren, die im konkreten Fall erforderlich sind oder aufgrund einer bewussten Entscheidung anderen Identitäten zugänglich gemacht werden sollen (Need to Know-Prinzip). Das auf Datensicherheit zielende Design von Gerätekomponenten kann auch unmittelbar dazu beitragen, im Sinne des Datenschutzrechts festgelegte Datenerhebungs- und -verarbeitungszwecke technisch abzusichern.
    - Es muss bereits hardwareseitig unveränderlich implementiert sein, dass vernetzte Geräte nur konkret definierte Funktionen ausführen können. So muss durch den Einsatz von „**Secure Elements**“ (also bestimmten Hardwarekomponenten) sichergestellt sein, dass unabhängig von der verwendeten Software, ein Missbrauch des Gerätes und seiner Funktionen ausgeschlossen ist.

- **Privacy by Design** – Allen in dem Internet der Dinge agierenden Personen – gleich, ob Bürger/-innen oder Unternehmen – muss die Möglichkeit verschafft werden, selbst darüber zu bestimmen, was mit den von ihnen erzeugten Daten passiert und zu welchen Zwecken dies geschehen soll. Die wichtigste Voraussetzung hierfür ist Transparenz und technologischer Schutz vor Missbrauch. Erst hierdurch wird im IoT auch die wirksame Durchsetzung geltender Prinzipien des **Datenschutzrechts** (Datensparsamkeit; Implementierung technischer Maßnahmen zum Schutz personenbezogener Daten) ermöglicht. Privacy by Design wird auch in der kommenden EU-Datenschutz-Grundverordnung (dort derzeit Art. 23 des Entwurfs) eine wesentliche Verpflichtung der verantwortlichen Stellen für die Datenverarbeitung sein.

III. Die Ausgangslage

1. Internet der Dinge – Was ist das?

Im Internet der Dinge werden in Zukunft alle möglichen elektronischen Geräte mit anderen elektronischen Geräten vernetzt. Prinzipiell kann das für jeden Gegenstand zutreffen (z.B. Kfz, Haushaltsgeräte, Produktionsmaschinen).

Das betrifft nicht nur den einzelnen Bürger, der in Zukunft auf dem Heimweg über seine App die Heizung regulieren kann oder über seine intelligente Uhr medizinische Daten an seine Versicherung übermitteln möchte, sondern auch die Produkte sowie die Entwicklungs-, Produktions- und Vertriebsprozesse der Wirtschaft selbst, etwa wenn Roboter in der Fahrzeugfertigung untereinander Daten austauschen.

2. Chancen – aber auch Risiken

Die Digitale Agenda definiert „Smart Cities“ als notwendige Bestandteile einer modernen und leistungsfähigen digitalen Infrastruktur wie „*die automatische Identifizierung in der Binnenschifffahrt, die*

digitale Planung in der Baubranche, die intelligente und leistungsfähige Anbindung von Häusern und die Vernetzung innerhalb der Gebäude und auch weitere Ansätze für eine integrierte nachhaltige Stadtentwicklung auf der Ebene städtischer Räume". Die Bundesregierung erkennt in diesem Anwendungsbeispiel eine große Chance für alle Beteiligten im Internet der Dinge. Bürgerinnen und Bürger können ihren Energieverbrauch senken, ihre Gesundheit mittels Ferndiagnose medizinischer Daten kontrollieren lassen oder in einer „Smart City" Unfallrisiken durch autonom fahrende Fahrzeuge senken. Unternehmen sparen Kosten bei Produktionsprozessen, verbessern die Datenbasis für Entwicklungsvorhaben und optimieren ihre Services für die Kunden.

Dennoch besteht Konsens, dass mit der Vernetzung im Internet der Dinge eine signifikante Erhöhung von Sicherheitsrisiken verbunden ist. Über 50 Prozent der Mittelständler sehen Risiken der IT Sicherheit als Bedrohung und damit als Eintrittsbarriere für ihr Industrie 4.0-Engagement.[3]

- Es werden mehr Angriffspunkte existieren, da mehr Kontaktpunkte in das Netz selbst bestehen. Es sind zudem Geräte und Verbindungen zu sichern, die heute mangels Verbindung noch nicht zu sichern sind bzw. bislang nicht gesichert werden mussten.
- Durch die Vernetzung der Beteiligten erhöht sich die Wahrscheinlichkeit von Identitätsdiebstählen und –missbrauch signifikant, und die Folgen entsprechender Vorfälle sind potentiell schwerwiegender.
- Die ansteigende Zahl vernetzter Geräte und vor allem auch die Tatsache, dass in Zukunft eine Vielzahl von Geräten mit IoT-Konnektivität Funktionen ausführen werden, ohne dass sie im Einzelnen bewusst und differenziert von Menschen gesteuert werden, erhöht die Anforderungen an den Funktionsschutz der Geräte selbst, auch gegen Angriffe von innen. Wenn nicht durch Secure Elements von vornherein sichergestellt ist, dass ein Gerät auch wirklich nur die Funktionen ausführt, für die es bestimmt ist, und nur die Daten erhebt und verarbeitet, die es erheben und verarbeiten soll, wird der Kontroll- und Sicherheitsaufwand nicht mehr zu leisten sein.
- Es wird größere Datenmengen und wesentlich mehr aus diesen Daten zu gewinnende Informationen geben. Hinzu kommt die Möglichkeit der Korrelation dieser Daten, woraus neue, bislang nicht mögliche Erkenntnisse aus hochsensiblen, vertraulichen Daten gewonnen werden können („Big Data").

Diese Risiken sind real und können lebensbedrohlich werden.

- So ist es jüngst einem IT-Spezialisten gelungen, ein Narkosegerät zu hacken. Über den hierfür eingesetzten Laptop war es möglich, die Steuerung des Medizingeräts zu übernehmen, die Beatmung zu stoppen und sogar alle Funktionen des Gerätes zu blockieren.[4] Auch ein Infusionsgerät konnte erfolgreich übernommen werden, mit der Folge, dass die Hacker etwa die Dosierung von Medikamenten ändern konnten.[5]
- Wiener Sicherheitsexperten konnten erfolgreich auf vernetzte Glühbirnen und auch Türschlösser zugreifen.[6]
- In den USA ist es IT-Forschern gelungen, Bremsen eines Corvette-Sportwagens von einem Smartphone aus abzuschalten. Als Einfallstor diente eine Schwachstelle in dem Telematik-Gerät einer US-Versicherung.[7]

Aus den IT-Sicherheitsrisiken erwachsen weitere, damit verbundene Risiken für den Schutz personenbezogener Daten einerseits und für den Schutz von Know-how/Geschäftsgeheimnissen sowie der Betriebssicherheit in Unternehmen andererseits. Der Erfolg des Internets der Dinge und die Akzeptanz bei Bürgern und Wirtschaft werden entscheidend davon abhängen, dass die Sicherheit in diesem hypervernetzten Umfeld gesetzlich verpflichtend und einheitlich auf struktureller Ebene sichergestellt wird. Hierfür braucht es ein **Identitätensicherheitsgesetz im Internet der Dinge**.

3. Risiken bislang gesetzlich nicht ausreichend adressiert

Die Risiken für die im Internet der Dinge miteinander verknüpften Identitäten sind nicht ausreichend gesetzlich adressiert; es fehlt den bestehenden gesetzlichen Regelungen insbesondere an einem **einheitlichen Schutzsubjekt: der IoT-Identität**.

- Die Datenschutzgesetze[8] zielen ausschließlich auf die Regelung des Umgangs mit personenbezogenen Daten ab; die IT-Sicherheit spielt lediglich eine Nebenrolle.
- Die aktuellen datensicherheitsrechtlichen Gesetze (bzw. Gesetzesvorhaben)[9] haben das Internet der Dinge nicht spezifisch im Blick und zielen nicht auf ein generell zu erreichendes IT-Sicherheitsniveau. In Ergänzung hierzu kann ein sektorenübergreifendes Identitätensicherheitsgesetz für den Schutz von vernetzten Geräten im allumfassenden Internet der Dinge sorgen.

Das IT-Sicherheitsgesetz dient – auch wenn der Name diese vermitteln könnte – keinen generellen IT-sicherheitsrechtlichen Zwecken, sondern ist ein Schutzgesetz für ausgewählte kritische Infrastrukturen: Der Gesetzgeber erkennt richtigerweise die IT-Infrastruktur von für das Gemeinwohl besonders relevanten Wirtschaftsbereichen (Elektrizität, Atomkraft, Transport und Verkehr, Gesundheit, Wasser) als schützenswert an. Um den erforderlichen und einheitlichen Schutz der IT-Infrastruktur dieser für die Gesellschaft elementaren Bereich sicherzustellen, verpflichtet es die Betreiber solch kritischer In frastrukturen, besondere Schutzmaßnahmen zu ergreifen. Denn die Funktionsfähigkeit des Staates hängt von der Verfügbarkeit dieser Infrastrukturbereiche ab. Es geht also bildlich gesprochen darum, dass nicht aufgrund von IT-Sicherheitsvorfällen halb Deutschland im Dunkeln liegt, nicht telefonieren kann oder kein Wasser mehr hat.

Aufgrund dieser spezifischen Zielrichtung erfolgt konsequenterweise auch die Umsetzung der gesetzlichen Vorgaben zur Implementierung technischer Sicherheitsvorkehrungen nur in einem beschränkten Lebens- bzw. Wirtschaftsbereich. Es sind, der Struktur und dem Ziel des IT-Sicherheitsgesetzes entsprechend, keine allgemein gültigen Regelungen zum hardwareseitigen Schutz von vernetzten Geräten und zum Schutz aller Identitäten im IoT vorgesehen.

Die Risiken des Internet der Dinge sind indes anders gelagert, denn das **Internet der Dinge ist ubiquitär**. Vernetzte Geräte werden in Zukunft in jedem Lebensbereich vorhanden sein. Entscheidend ist dabei die Sicherheit aller Anwender, die vernetzte Geräte einsetzen, egal ob dies in der Fabrik eines Unternehmens (Industrie 4.0) oder bei der Nutzung von IoT-Produkten (vernetztes Fahren, vernetzte Haushaltsgeräte etc.) erfolgt.

Den bestehenden Gesetzen und legislativen Vorhaben mangelt es folglich an dem für die Regulierung des Internets der Dinge so wichtigen technologie- und interessenneutralen Ansatz, der auf struktureller Ebene den Schutz von Identitäten sowie die Sicherheit von Datenerzeugung und -übermittlung in einer vernetzten Welt branchenneutral in den Mittelpunkt stellt. So vielfältig und zufällig die Anwendungsbereiche des Internets der Dinge sind, so generell und allgemein verbindlich sollten daher die gesetzlichen Mindestvoraussetzungen an ein in Verkehr bringen von sicheren Geräten sein. Eine Differenzierung nach für das Allgemeinwohl wichtigen oder unwichtigen Infrastrukturen als „Momentaufnahme“ kann aufgrund der Ubiquität und der hohen Veränderungsdynamik des IoT für den hardwarebasierten Schutz der vernetzten Identitäten keine Rolle spielen.

IV. Die notwendigen Maßnahmen

Für eine effiziente und nachhaltige Entwicklung des IoT in Deutschland und Europa, die auf Vertrauen, Transparenz, Planungs- und auf Rechtssicherheit beruht, mangelt es bisher an branchenübergreifenden Pflichten, die ein **zertifiziertes Sicherheitsniveau auf struktureller und technischer Ebene der vernetzen Geräte** verlangen. Es geht um das Vertrauen in die Integrität der Daten, der Funktonen der vernetzten Geräte sowie ihrer Kommunikation mit anderen vernetzten Geräten. Ein Gesetz kann diese Lücke schließen, indem es den notwendigen technischen Schutz der Bezugspunkte eines jeden intelligenten Gerätes in den Mittelpunkt stellt und einen neuen regulatorischen Ansatz wählt: die **Sicherheit der Identität**. Das Gesetz regelt dabei, welche Voraussetzungen Hersteller von intelligenten, vernetzten Geräten zu erfüllen haben, um die Geräte auf dem deutschen bzw. europäischen Markt in Verkehr zu bringen:

- **Security by Design**

  Essentieller Ansatzpunkt des regulatorischen Konzepts des **Identitätensicherheitsgesetzes im Internet der Dinge** ist eine **zertifizierte Sicherheitsstruktur ab Werk**. Hierzu gehört die Pflicht zur **Verschlüsselung** sowohl der Informationen zur Identität (und ggf. weiterer Angaben) in dem Gerät als auch der Übermittlungswege. Eine effektive **Authentifizierung** der Identitäten untereinander muss ermöglicht werden. Diese Voreinstellungen sollten technologie- bzw. anwendungsoffen konzipiert sein, um Lock-in-Effekte zu vermeiden. Auch muss es den Beteiligten ermöglicht werden, die für den jeweiligen Zweck erforderlichen **Sicherheitslevel** festlegen zu können. Zudem ist sicherzustellen, dass alle Beteiligten auf die so beschriebenen Standards und deren Einhaltung vertrauen können. Der Funktionsumfang vernetzter Geräte muss in der Hardware unveränderlich festgelegt werden und dem Zugriff und dem Missbrauch durch unberechtigte Dritte entzogen sein. Die technische Struktur von IoT-Geräten muss es ermöglichen, dass Identitäten nur der Zugriff auf solche Daten erlaubt wird, die in der konkreten Verarbeitungssituation erforderlich sind, und dass nur diejenigen Daten erzeugt bzw. erhoben werden, die zum betreffenden Zeitpunkt für die Anwendung notwendig sind (**Need to Know-Prinzip**).

  So sollte nur das für die Abrechnung zuständige Unternehmen Abrechnungsdaten von Smart Services entschlüsseln können. Ebenso sollte eine Produktionsmaschine nur die für ihren Produktionsschritt notwendigen Daten nutzen können. Die für die Umsetzung solcher Anforderungen erforderliche Technologie gibt es bereits. Kurzum: Sicherheit muss ab Werk in den Geräten verankert werden, und die Umsetzung auf Produktebene muss durch existierende, bewährte und als „State of the Art“ anerkannte **Zertifizierungen** geprüft und bestätigt werden.

- **Privacy by Design**

  Neben den sicherheitstechnischen Pflichten haben Hersteller von intelligenten Geräten durch unveränderliche, in den Geräten zu verbauende Komponenten vorzusehen, dass allein eine berechtigte Entität, insbesondere der Nutzer des Gerätes, die Möglichkeit zur Veränderung der herstellerseitig vorgesehenen **Parametrisierung** (im Sinne eines Rechtemanagements für den Zugriff auf Daten) innerhalb des Gerätes besitzt. Damit wäre es möglich, zukunftsfest und flexibel festzulegen, welche Identität welche Anforderungen zu erfüllen hat. Daneben könnten die Beteiligten bestimmte Daten mit **Zweckangaben** versehen, so dass der Zugriff auf Daten technisch reguliert werden kann. Hinzu kommt: Bei der IT-Sicherheit auf Strukturebene anzusetzen, bietet die große Chance, die Ziele des **Datenschutzes** (Datensparsamkeit, Begrenzung der Datenverarbeitung auf das erforderliche Maß gemäß den zulässigen und festgelegen Zwecken, Kontrolle, Transparenz und Wahlmöglichkeiten für die Betroffenen) zu fördern.

Nur eine Lösung, die bei jeder einzelnen Identität (Mensch oder technische Einheit) ansetzt, stellt sicher, dass Regeln und Maßnahmen für die Sicherheit und Integrität von IKT-Systemen technologie- und damit interessen- und produktneutral auf einer Ebene umgesetzt werden können, die echte und

anerkannte Sicherheit bietet. Das ist auch der Weg, der in Deutschland und der EU bereits erfolgreich beschritten wurde. Beispiele sind der elektronische Personalausweis oder Sicherheitschips auf Kreditkarten.

Eine rein software-basierte Lösung kann diese Anforderungen nicht erfüllen. Jede Software, und sei sie aktuell und gut gesichert, ist ihrer Natur nach angreifbar. Nur ein Beispiel: Jüngst warnte etwa ein internationaler Hersteller von Routern vor Hackerangriffen, bei denen manipulierte Firmware auf die Geräte gespielt wird.[10] Es gibt keine nur auf Basis von Software **zertifizierte** und als sicher **testierte** Lösung. Dem entsprechend kann Software auch von vornherein nicht als Mittel eines effektiven Schutzes vernetzter Geräte im IoT dienen. Vielmehr ist es erforderlich, den bereits in Teilbereichen, wie etwa dem elektronischen Personalausweis oder bei Kreditkarten, stattfindenden Einsatz von **Secure Elements**, also von sicheren und vertrauenswürdigen Hardwarekomponenten gesetzlich vorzuschreiben.

Wenn dieses Grundprinzip gesetzlich umgesetzt wird, können die erforderlichen technischen Regeln und Standards durch dafür zuständige – und zumeist bereits etablierte – Gremien oder Behörden ermittelt und zertifiziert werden. Beispielhaft für eine solche Stelle sei das Bundesamt für Sicherheit in der Informationstechnik („BSI“) genannt, das im Bereich vernetzte Systeme bereits vergleichbare Aufgaben für RFID-Technologie (Access Control) und Smart Meter Gateway-Sicherheitsmodule erfolgreich erfüllt. Auch in anderen EU-Mitgliedstaaten und auf europäischer Ebene selbst existieren entsprechend qualifizierte und mit der erforderlichen Erfahrung ausgestattete Behörden, so etwa in Frankreich die „Agence nationale de la sécurité des systèmes d'information“ (ANSSI) oder auf EU-Ebene die „Europäische Agentur für Netz-und Informationssicherheit“ (ENISA). Zudem können durchaus auch private Stellen das Einhalten technischer Vorgaben prüfen; wenn diese Stellen entsprechend staatlich geprüft und akkreditiert sind. Ein Beispiel hierfür ist etwa die qualifizierte elektronische Signatur: Die Bundesnetzagentur prüft private Zertifizierungsanbieter und erteilt nach erfolgreicher Prüfung ein Gütesiegel, mit dem der Nachweis der umfassend geprüften technischen und administrativen Sicherheit des Anbieters zum Ausdruck gebracht wird. Der Anbieter wiederum reicht dann die sicheren Zertifikate an Bürger und Unternehmen aus.

V. Konkret – Die Umsetzung

Vor diesem Hintergrund ist es notwendig, ein neues Identitätensicherheitsgesetz für das Internet der Dinge zu schaffen. Das allgemeine **Ziel dieses Gesetzes** könnte in der Gesetzesbegründung wie folgt umschrieben werden:

> *„Technische, auf Hardwareebene implementierte Mindestanforderungen für die Kommunikationseinheiten des Internets der Dinge zur Gewährleistung von eineindeutigen **Identitäten**, **Datenschutz**, **Informationssicherheit** und **Interoperabilität** zu normieren.“*[11]

Das Gesetz würde die Grundlage für Rechts- und Planungssicherheit in Wirtschaft und Gesellschaft schaffen und damit den notwendigen Impuls dafür setzen, dass Deutschland und Europa das Internet der Dinge bzw. das Thema Industrie 4.0 als Wachstumsmotor nutzen und zukunftsfeste Arbeitsplätze schaffen kann.

1. Legislative Ebene

1.1 Europäische Union

Idealerweise sollte die Umsetzung des Identitätensicherheitsgesetzes im Internet der Dinge auf europäischer Ebene erfolgen. Der Vorteil einer Verankerung auf EU-Ebene durch eine Verordnung, notfalls auch durch eine Richtlinie mit Umsetzung durch die Mitgliedsstaaten, besteht darin, verbindlich im gesamten Unionsgebiet einheitliche Vorgaben für vernetzte Geräte im Internet der Dinge zu etablieren und damit ein international anzuerkennendes **„Level Playing Field“** zu schaffen. Gerade auf EU-Ebene hat sich in der Vergangenheit gezeigt, dass effizient Mindestanforderungen an bestimmte Produkte und eine einheitliche Überwachung des Sicherheitsstandards im gesamten Markt der Europäischen Union durchgesetzt werden können. So wurden etwa mit der Verordnung 2008/765/EG (die Grundlage der CE-Kennzeichnung ist) verbindliche Vorgaben zur Kontrolle von auf den Gemeinschaftsmarkt eingeführten Produkten festgelegt. Danach haben die Mitgliedstaaten sicherzustellen, dass Produkte, die eine ernste Gefahr darstellen, was ein rasches Eingreifen erforderlich macht – einschließlich einer ernsten Gefahr ohne unmittelbare Auswirkung, zurückgerufen oder vom Markt genommen werden.

Es existieren auch bereits europäische Vorgaben zur Sicherheit von vernetzten Geräten. So sieht die **Energieeffizienz-Richtlinie**[12] vor, dass Mitgliedstaaten die Sicherheit von intelligenten Verbrauchszählern und der Datenkommunikation sowie die Wahrung der Privatsphäre der Endkunden im Einklang mit den einschlägigen Rechtsvorschriften der Union über den Datenschutz und den Schutz der Privatsphäre zu gewährleisten haben (vgl. Art. 9 Abs. 2 Buchst. b RL 2012/27/EU). Umgesetzt werden sollen diese Vorgaben in Deutschland unter anderem durch die geplante Messsystemverordnung (**MsysV**), die auf der Ermächtigungsgrundlage von § 21i Abs. 1 Nr. 12 Energiewirtschaftsgesetz (EnWG)[13] zum Erlass einer entsprechenden Rechtsverordnung beruht. Das EnWG schreibt zur Gewährleistung von Datenschutz, Datensicherheit und Interoperabilität bestimmte technische Voraussetzungen für vernetzte Messsysteme vor, einschließlich eines Zertifizierungsverfahrens um das Erfüllen der Voraussetzungen sicherzustellen.

Es wird eine Lösung anzustreben sein, die für den gesamten Binnenmarkt gilt und auf internationaler Ebene, dem **globalen Markt** des Internet der Dinge, ihre volle Wirkung entfalten kann. Ein solcher unionrechtlicher Vorstoß auf dem Gebiet der IKT-Sicherheit kann zudem für eine Aufwertung des **Wirtschaftsstandorts Europa** für sichere Technologien der Zukunft im Vergleich zu anderen Nationen sorgen.

1.2 Bundesrecht

Eine Regelung auf europäische Ebene ist nicht zuletzt auch deshalb grundsätzlich vorzugswürdig, weil ein rein mitgliedsstaatliches Verbot mit Blick auf die geltende europäische Warenverkehrsfreiheit auf seine Rechtfertigung hin zu prüfen wäre. Das Verbot für Hersteller, Importeure und Händler, keine den Voraussetzungen des Gesetzes nicht entsprechenden Geräte in den Verkehr zu bringen, berührt die in dem Vertrag der Arbeitsweise der Europäischen Union geregelte (vgl. Art. 28 – 37 AEUV) Warenverkehrsfreiheit und beschränkt diese für Gerätehersteller, Importeure und Händler aus anderen EU-Mitgliedstaaten. Auf der anderen Seite ist eine Beschränkung der Warenverkehrsfreiheit aber auch nicht per se verboten. Sie unterliegt vielmehr einem Rechtfertigungsvorbehalt nach Art. 36 AEUV. Eine Beschränkung der Warenverkehrsfreiheit ist etwa aus Gründen der öffentlichen Sittlichkeit, Ordnung und Sicherheit und/oder zum Schutz der Gesundheit und des Lebens von Menschen erlaubt. Von solchen Gründen kann man durchaus gewichtige anführen, wenn es um die Sicherheit des Internets der Dinge geht.

Als Vorstufe zu einer EU-weiten Regelung kann damit auch eine bundesgesetzliche Verabschiedung eines entsprechenden Gesetzes in Betracht kommen. Ein solches Bundesgesetz hätte den Vorteil, dass mit einer schnelleren Verabschiedung als auf europäischer Ebene gerechnet werden kann. Ein solches

Bundesgesetz könnte zudem unproblematisch auf die bereits bekannte Systematik des EnWG zurückgreifen (s.o.). Durch ein Bundesgesetz können die Prinzipen von „Security by Design“ und „Privacy by Design“ verankert werden, indem technische Mindeststandards für die Sicherheitsstruktur von Geräten für das Internet der Dinge vorgesehen werden. Die technische Ausgestaltung und Zertifizierung kann entsprechenden Gremien oder Fachbehörden überlassen bzw. übertragen werden (vgl. unter V. 3. 3.2).

2. Art des Gesetzes

Um sicherzustellen, dass tatsächlich nur hardwareseitig gesicherte, den gesetzlichen Mindestanforderungen genügende Produkte auf den Markt gelangen, sollte das Identitätensicherheitsgesetz in der Form eines **Verbotsgesetzes mit Erlaubnisvorbehalt** aufgebaut werden. Dies bedeutet, dass vernetzte Geräte für das Internet der Dinge **nur dann in Verkehr gebracht werden dürfen, wenn** die inhaltlichen Mindestanforderungen (siehe dazu unter V. 3.) erfüllt sind.

Diese Regelungssystematik ist Standard in der EU wie auch in Deutschland. Zum Beispiel sind nach der geltenden Datenschutzrichtlinie (vgl. Art. 7 Richtlinie 1995/46/EG) Datenverarbeitungen nur zulässig, soweit eine Rechtsvorschrift dies erlaubt, der Betroffene eingewilligt hat oder ein weiterer, abschließend benannter Erlaubnistatbestand vorliegt. Eine weitere Parallele lässt sich zum EnWG ziehen. Nach § 21e Abs. 4 S. 1 EnWG dürfen etwa in Gebäuden, die neu an das Energieversorgungsnetz angeschlossen werden, nur Messeinrichtungen zur Erfassung elektrischer Energie eingebaut werden, bei denen die Einhaltung der Anforderungen des Schutzprofils in einem Zertifizierungsverfahren zuvor festgestellt wurde. Nach § 21e Abs. 1 EnWG dürfen nur Messsysteme verwendet werden, die den eichrechtlichen Vorschriften entsprechen. Gerade die Parallelität der Vorgaben des EnWG mit den hier vorgeschlagenen Regelungen verdeutlicht, dass der Gesetzgeber im Bereich des Inverkehrbringens intelligenter Geräte bereits derzeit davon ausgeht, dass die Ausgestaltung der relevanten Vorschriften in Form von Verbotsnormen mit Erlaubnisvorbehalt das adäquate Mittel ist, um die technische Sicherheit vernetzter Geräte und damit des gesamten Internets der Dinge, die Datenintegrität und auch den Datenschutz bei der Nutzung solcher vernetzter Geräte sicherzustellen.

Diese bereits in Einzelbereichen bewährte Regelungssystematik kann nun durch das Identitätensicherheitsgesetz auf eine übergeordnete Ebene gehoben werden.

3. Inhaltliche Anforderungen

3.1 Zwingende Mindestanforderungen

Hersteller, Importeure, Händler oder sonstige Personen, die vernetzte Geräte für das Internet der Dinge in Verkehr bringen, haben nach den Vorgaben des Identitätensicherheitsgesetzes sicherzustellen, dass durch eine Verwendung von Secure Elements in der **Hardware der Geräte**

- die **eineindeutige Identität** des IoT- Gerätes festgelegt ist.

  Erläuterung: Durch die eineindeutige Identität des Geräts soll die Herkunft des Gerätes nachvollziehbar und nachweisbar werden. Die Authentizität des Geräts muss jederzeit gewährleistet sein.

- die Kommunikation mit anderen IoT-Geräten und die Datenverarbeitung standardisiert stets über einen **verschlüsselten**, **integritätsgesicherten** Kanal erfolgt.[14]

  Erläuterung: Der Einsatz von Verschlüsselungstechniken muss, wie auch im Entwurf zur

MsysV für intelligente Messsysteme, zum Standard beim Einsatz von vernetzten Geräten gehören. Daher muss eine Pflicht bestehen, dass Geräte hardwareseitig nur verschlüsselt mit Daten umgehen. Die konkrete Form der Verschlüsselung sollte dem Stand der Technik (vgl. unter V. 3. 3.2) überlassen sein.

- unveränderlich festgelegt ist, dass nur ein oder mehrere definierte **Berechtigte** Zugriff auf die Hardware nehmen dürfen.

  Erläuterung: Beim Einsatz vernetzter Geräte müssen Anwender davon ausgehen können, dass allein die Berechtigten (Hersteller, Nutzer, o.ä.) Zugriff auf die Hardware und die Einstellungen des Geräts haben. Die Festlegung der Berechtigten muss unveränderbar sein. Vergleichend sei hier auf den Entwurf der MsysV verwiesen, nach dem bereits durch die technische Ausstattung des Smart Meter Gateway gesichert sein muss, „*das ein direkter Zugriff auf dieses nur durch eine einzige Instanz, nämlich dem Smart Meter Gateway Administrator, möglich ist*“.[15]

- festgelegt ist, **welche andere Identität** mit dem Gerät **kommunizieren** darf, eine gegenseitige **Authentisierung** der Kommunikationspartner erforderlich ist[16] und nur die Berechtigten diese Einstellungen ändern und bestimmen können.

  Erläuterung: Das Internet der Dinge lebt von der Vernetzung verschiedener Identitäten. Um das Vertrauen in die vernetzte Alltags- und auch Wirtschaftswelt zu stärken, muss gesetzlich gesichert und auf Hardwareebene unveränderlich vorgesehen sein, dass nur berechtigte und authentisierte Identitäten miteinander kommunizieren können. Ein Eindringen von unberechtigten Dritten, z.B. Hackern, wird damit ausgeschlossen.

- festgelegt ist, welche Funktionen das Gerät besitzt, welche Datenerhebungen und -verarbeitungen erfolgen können, an welche Geräte Daten übermittelt werden und allein die Berechtigten die Möglichkeit besitzen, dies zu ändern.

  Erläuterung: Nutzer von vernetzten Geräten müssen darauf vertrauen können, dass ihr Gerät“ nur jene Funktionen ausführt und auch nur in diesem Rahmen Daten erhebt und verarbeitet, die auch tatsächlich von den Berechtigten gewollt und vorgesehen sind. Jede mit diesen Vorgaben nicht vereinbare Funktion und Datenverarbeitung ist bereits hardwareseitig ausgeschlossen.

- unveränderlich **Zweckfelder** vorgesehen sind, mit Hilfe derer allein die Berechtigten bestimmen können, zu welchen Zwecken bestimmte Daten aus dem vernetzten Gerät von autorisierten Dritten verwendet werden dürfen.

  Erläuterung: Für die Berechtigten muss die Möglichkeit bestehen, in vorhandenen Zweckfeldern unveränderlich zu bestimmen, wofür Daten aus dem vernetzten Gerät verwendet werden dürfen. Diese Möglichkeit muss nicht genutzt werden; wenn sie aber genutzt wird, dürfen die festgelegten Zwecke nicht von Dritten verändert werden können.

3.2 Beachtung des Stands der Technik

Ziel der gesetzlichen Vorgaben sollte sein, dass vernetzte Geräte stets dem **Stand der Technik** („**State of the Art**“) entsprechen. Was der jeweils gültige Stand der Technik ist, sollte durch dritte, mit entsprechendem Fachwissen ausgestattete Stellen festgelegt werden. Dem Stand der Technik entspricht ein sicheres Gerät zum Beispiel dann, wenn es (in Anlehnung an bereits bekannte Regelungen, etwa im Bereich der Smart Meter Gateways) die Vorgaben von Schutzprofilen oder die in technischen Richtlinien niedergelegten technischen Mindestanforderungen erfüllt.[17]

Um der technologischen Entwicklung entsprechend stets **aktuelle Vorgaben** an den Stand der Technik zu machen, das System innovationsoffen zu halten und neuen Bedrohungslagen sprich Risiken entsprechende Weiterentwicklungen zu ermöglichen, kann sich das Identitätensicherheitsgesetz beispielsweise der vorgeschlagenen Verweisungstechnik des Entwurfs der MsysV (dort § 4 Abs. 2) bedienen. In diesem Fall sollte die jeweils geltende Fassung von zu beachtenden technischen Richtlinien im Bundesanzeiger durch Verweis auf die Internetseite des BSI bekannt gemacht werden.[18]

3.3 Informations- und Kennzeichnungspflicht

Daneben sind Hersteller, Importeure und Händler dazu verpflichtet, deutlich sichtbar und verständlich über die konkrete Umsetzung der oben benannten Mindestanforderungen zu informieren. Es geht dabei zum einen darum, auf oder im Zusammenhang mit dem Gerät darüber zu informieren, dass das Gerät den gesetzlichen Anforderungen entspricht. Dies kann ggf. durch ein entsprechendes **Kennzeichen** erfolgen. Zum anderen bezieht sich die gesetzliche **Informationspflicht** aber gerade auch auf die festgelegten Funktionen, Datenerhebungen und -verarbeitungen des vernetzten Gerätes und die Berechtigung(en) für den Zugriff auf die Einstellungen. Denn erst wenn der Anwender weiß, was ein Gerät bestimmungsgemäß tut und wer in welcher Hinsicht berechtigt ist, Daten mit dem Gerät auszutauschen und ggf. auf das Gerät zuzugreifen, kann er eine informierte Entscheidung über die Anschaffung bzw. den Betrieb des Geräts treffen.

4. Rechtsfolgen

Wie in vergleichbar konzipierten Gesetzen kann auch das Verbot im Identitätensicherheitsgesetz vom Staat durchgesetzt und entsprechende Verstöße verfolgt werden. Daneben kann als indirekt wirkendes Steuerungsinstrument auch Wettbewerbern die Möglichkeit eröffnet werden, gegen rechtswidrig handelnde Konkurrenten vorzugehen, um Wettbewerbsnachteile zu verhindern. Zuletzt sind auch Verbrauchern oder Unternehmen, die infolge von Verstößen gegen das Gesetz Schäden erleiden, effektive Unterlassungs- und Schadenersatzansprüche zur Verfügung zu stellen.

4.1 Ordnungswidrigkeiten / Straftatbestände

Das Identitätensicherheitsgesetz kann mindestens durch **Ordnungswidrigkeitstatbestände** bewehrt sein. Dabei sollte es keinen vorgegebenen Bußgeldrahmen geben. Vielmehr sollte die Höhe von **Bußgeldern** ähnlich wie in den Regelungen zur geplanten Datenschutz-Grundverordnung (DS-GVO)[19] vom weltweit erzielten Jahresumsatz des Herstellers, Importeurs bzw. Händlers abhängig gemacht werden. Diese Form der Vorgabe einer variablen maximalen Geldbuße ist auch bereits aus dem geltenden **Kartellrecht** auf nationaler und europäischer Ebene bekannt (vgl. § 81 Abs. 4 GWB und Art. 23 Abs. 1 Verordnung 1/2003/EG). Ein solch flexibler staatlicher Strafrahmen bietet den Vorteil, dass mit **verhältnismäßigen Bußgeldern** gegen Verletzer vorgegangen werden kann (diese die Bußgelder daher auch nicht ihrer Geschäftsmodelle gemäß „einpreisen“ können). Internationale Großkonzerne haben folglich Geldbußen in anderer Höhe zu erwarten als ein rein regional tätiges Unternehmen.

Besonders schwere Rechtsverletzungen, etwa solche, die vorsätzlich begangen werden, oder wiederholte Verstöße gegen das gesetzliche Verbot, sollten darüber hinaus auch als **Straftatbestände** ausgestaltet werden.

4.2 Wettbewerbsrecht

Das Wettbewerbsrecht bietet neben dem staatlichen Strafanspruch ein effektives Mittel, um gesetzeskonformes Marktverhalten zu bewirken. Zwar handelt es sich beim Wettbewerbsrecht um Zivilrecht: Wettbewerber erhalten ein Werkzeug, um gegen sich unlauter verhaltende Konkurrenten vorzugehen. Jedoch hat es sich gerade im letzten Jahrzehnt gezeigt, dass das Wettbewerbsrecht gerade in staatlich nur schwer zu kontrollierenden Marktbereichen viel bewirken kann. Man denke an den Online-Handel (Widerrufsbelehrungen, „Button-Lösung“ etc.) oder bestimmte Formen der aggressiven Werbung (Spam-E-Mails, unzulässige Telefonwerbung).

Verschafft sich ein Hersteller, Importeur oder Händler dadurch einen Vorteil am Markt, dass er vernetzte Geräte etwa billiger in Verkehr bringen kann, weil er die gesetzlichen Mindestanforderungen nicht erfüllt, so sollten Wettbewerber die Möglichkeit haben, dieses Marktverhalten abzumahnen und den Konkurrenten auf Unterlassung in Anspruch zu nehmen. Hierzu könnte sich ein betroffener Wettbewerber wohl auch ohne besondere gesetzliche Regelung auf § 4 Nr. 11 **UWG** stützen, wonach insbesondere unlauter handelt, wer einer gesetzlichen Vorschrift zuwiderhandelt, die auch dazu bestimmt ist, im Interesse der Marktteilnehmer das **Marktverhalten zu regeln**. Ob jedoch Vorschriften dazu bestimmt sind, das Marktverhalten zu regeln, stellt sich in der Praxis häufig als schwierige Auslegungsfrage dar, die dann gerichtlich zu klären ist. Um einer solchen Rechtsunsicherheit vorzubeugen, sollte zumindest in der Präambel und der Gesetzesbegründung zum Identitätensicherheitsgesetz klar zum Ausdruck gebracht werden, dass es sich bei den Mindestanforderungen an vernetzte Geräte um eine Vorschrift handelt, die im Interesse der Marktteilnehmer dazu bestimmt ist, das Marktverhalten zu regeln.

4.3 Unterlassungsklagengesetz

Die gesetzliche Vorgabe, allein sichere Geräte in Verkehr bringen zu dürfen, dient auch dem **Verbraucherschutz**, insbesondere dem Schutz und der Sicherheit personenbezogener Daten, und schafft Vertrauen in ein sich immer mehr vernetzendes Alltags- und Wirtschaftsleben. Für den einzelnen Betroffenen ist es jedoch häufig schwierig und mit erheblichen finanziellen Risiken behaftet, sich im Fall von Rechtsverletzungen allein gegen große internationale Unternehmen zur Wehr zu setzen. Ein effektives Mittel, um Verbraucherrechte auch gegenüber zwangsläufig Finanzstärkeren Geltung zu verschaffen, damit eine wichtige Ergänzung der Rechtsdurchsetzung, stellt das Klagerecht von Verbänden nach dem **Unterlassungsklagengesetz** (UKlaG) dar. Der Verbraucherzentrale Bundesverband e.V. (VZBV) konnte mit diesem Instrument in den letzten Jahren Verbraucherrechte gegenüber Großkonzernen wie Samsung und Google effektiv gerichtlich durchsetzen.[20] Aus diesem Grund plant die Bundesregierung derzeit auch speziell im Bereich des Datenschutzrechts, ein **Verbandsklagerecht** bei Datenschutzverstößen einzuführen.[21] Und auch auf europäischer Ebene soll in der geplanten DS-GVO vorgesehen werden, dass Mitgliedstaaten nationale Vorgaben für ein solches Verbandsklagerecht bei Datenschutzverstößen erlassen können.[22]

Mit Blick auf das Identitätensicherheitsgesetz sollte daher über eine Erweiterung des § 2 Abs. 2 UKlaG nachgedacht werden und die Rechtsvorschriften zum Verbot des Inverkehrbringens von den Mindestanforderungen und dem Stand der Technik nicht entsprechenden Geräten in den Katalog von Verbraucherschutzgesetzen aufgenommen werden.

4.4 Ansprüche von Unternehmen und Verbrauchern

Gerade im Bereich vernetzter Maschinen (Industrie 4.0) kann ein nicht autorisierter Zugriff auf Geräte und eine missbräuchliche Stilllegung[23] oder Umprogrammierung der Funktionen zu beträchtlichen Schäden führen. Aber auch einzelne Verbraucher können geschädigt sein. Wenn einem einzelnen Betroffenen, also einer natürlichen Person oder auch einem Unternehmen, infolge des Inverkehrbringens eines vernetzten Geräts, welches nicht den gesetzlichen Anforderungen entspricht, ein Schaden entsteht, muss der Betroffene daher die Möglichkeit haben, einen entsprechenden **Schadensersatz**- sowie gegebenenfalls auch noch einen **Unterlassungs**- und/oder **Beseitigungsanspruch** gegen den Verletzer geltend zu machen.

Oft ist es für Betroffene jedoch schwierig, kostenintensiv und in der Folge risikoreich, einen Schadenersatzanspruch tatsächlich durchzusetzen. Problematisch ist gerade im Bereich einer Haftung für fehlerhafte Produkte sehr häufig, dem Hersteller, Importeur oder Händler (je nachdem, wer das Gerät in Verkehr gebracht hat) ein Verschulden nachzuweisen, wie es im einfachen Schadensersatzrecht des deutschen Zivilrechts grundsätzlich notwendig ist. Um Betroffenen in diesen Fällen die Durchsetzung von Schadensersatzansprüchen zu erleichtern, gibt es die verschuldensunabhängige Produkthaftung. Nach § 1 Abs. 1 S. 1 **Produkthaftungsgesetz** (ProdHaftG) ist u.a. der Hersteller eines fehlerhaften Produkts verpflichtet, dem Geschädigten den daraus entstehenden Schaden zu ersetzen. Er ist zum Schadenersatz verpflichtet, da das Produkt in der konkreten, fehlerhaften Form gar nicht in Verkehr gebracht hätte werden dürfen. Diese Herangehensweise lässt sich auf das Inverkehrbringen von sicheren Geräten für das IoT übertragen. Den gesetzlichen Mindestanforderungen nicht genügende und dem Stand der Technik nicht entsprechende Geräte dürfen nicht in Verkehr gebracht werden. Ein sich aufgrund der mangelnden Sicherheit des vernetzten Gerätes realisierender Schaden ist durch den Hersteller – bzw., je nach Konstellation, (auch) durch den Importeur oder Händler – zu ersetzen, es sei denn er kann nachweisen, dass er für den Fehler nicht verantwortlich ist (vgl. hierzu die Regelungen des § 1 Abs. 2 ProdHaftG).

VI. Fazit

Unsere Gesellschaft steht vor einem disruptiven technologischen Wendepunkt. Bisher ist kaum absehbar, was die Hypervernetzung unseres Alltags- und der Geschäftswelt für die Interaktion der rechtlichen Akteure bedeutet. Klar ist jedoch: Es braucht Regeln, die zukunftstauglich sind. „Security by Design“ bzw. „Privacy by Design“ als struktureller Ansatz ist der richtige Weg, da er den Menschen und die mit ihnen verbundenen Identitäten in den Mittelpunkt stellt.

Der Grundgedanke von der Sicherheit vernetzter Geräte und die zu ergreifenden Maßnahmen sind dem deutschen Gesetzgeber bereits aus sektorenspezifischen Regelungsbereichen, wie etwa dem EnWG und dem zugehörigem Entwurf der Messsystemverordnung, bekannt:

> *„Ein leistungsfähiges intelligentes Netz erfordert daher sichere IT- und TK- Technologien bereits auf Ebene der Datenerfassung und ersten Weiterverteilungsstufe, dem Smart Meter Gateway, das als Kommunikationseinheit in der Sicherheitsarchitektur eines intelligenten Messsystems die Schlüsselrolle einnimmt“.*[24]

Diese Schlüsselrolle spielt im zukünftigen, allumfassenden Internet der Dinge die durch das Identitätensicherheitsgesetz adressierte Identität.

Für den Erfolg jedweden Gesetzesvorhabens wird es darauf ankommen, dass dieses schnell in Angriff genommen und umgesetzt wird. Denn die technologische Entwicklung schreitet rasant voran und wird derzeit beinahe ausschließlich von Big Data-Unternehmen vorangetrieben, die IT-Sicherheit nur im eigenen Interesse betreiben und an grundlegenden Standards, die Bürgerinnen und Bürger sowie die

Wirtschaft insgesamt schützen können, wenig Interesse haben. Die so entstehenden de facto-Standards sind später, wenn sie einmal etabliert sind, kaum mehr beeinflussbar. Ein fokussiertes und schlankes Gesetz kann diese am Gemeinwohl wenig orientierten de facto-Standards nicht nur verhindern, sondern vielmehr einen eigenständigen und einen prosperierenden Markt für Privacy- und Security-freundliche Innovationen schaffen.

Die deutsche Sicherheitsindustrie hat eine ihrer Stärken in der Entwicklung und Umsetzung von Systemen, die – basierend auf speziellen sicherheitszertifizierten Lösungen – Schutz vor Angriffen für den Zahlungsverkehr, für hoheitliche Dokumente, Smartphones und Secure Gateways bieten. Deutschland ist also für die Einführung von Security-Standards gut gerüstet, und die europäische Wirtschaft hätte einen Startvorteil im Wettbewerb um innovative Produkte.

Neben den einzelnen Bürgerinnen und Bürgern und den Sicherheitstechnologien entwickelnden Unternehmen würde auch die hiesige Wirtschaft generell von einer grundlegenden IT-Sicherheit im Internet der Dinge profitieren. Gerade deutsche Unternehmen sind jeden Tag Ziel von Industriespionage sowohl von privater als auch von drittstaatlicher Seite. Vor diesem Hintergrund stellt das IoT und die damit einhergehende Vernetzung aller Geräte ein Risiko für Unternehmen und Gesellschaft dar. Allgemein verbindliche Sicherheitsstandards sind hier ein bewährtes Mittel. So kann der strukturelle Ansatz nicht nur Innovationstreiber, sondern für viele Unternehmen auch Grundvoraussetzung für die Einführung neuer Technologien sein:

- Eine durchgängige, intelligente und kryptografische **Security-Architektur** ermöglicht es Deutschland und Europa, eigene Kontrollpunkte zu setzen und ungeschützten Datenabfluss zu bremsen. Auch die Digitale Agenda der Bundesregierung fordert, dass wir „*unsere technologische Systemkompetenz erweitern und Abhängigkeiten reduzieren*“ müssen.
- Die **Systembeherrschbarkeit** ist unabdingbar, wenn es darum geht, mit neuen Technologien zu arbeiten – und zwar von Anfang an als Innovationstreiber und nicht erst, wenn sich die Technologien anderswo durchgesetzt haben. Ohne Systembeherrschbarkeit ist Vertrauen nicht herstellbar.
- Es muss **Transparenz** der technischen Architektur und der Datenflüsse geschaffen werden.
- **Rechtssicherheit**: Das Rechtssystem muss, damit es überhaupt relevant bleiben kann und nicht der Eindruck entsteht, man befinde sich im sprichwörtlichen wilden „Cyber-Wildwest“, möglichst von Anfang die Realität regulieren.
- Wenn Unternehmen zukünftig Sicherheitsvorkehrungen treffen, die gesetzlichen Mindeststandards folgen, **spart das Kosten** für die Allgemeinheit. Bislang muss die Gesellschaft für Schäden bezahlen, wenn Unternehmen Investitionen in digitale Sicherheit unterlassen.
- Verbrauchern kann die **Kontrolle** über von ihnen erzeugte Daten zurückgegeben werden. Daher muss bereits beim Netzzugang eine nicht verletzbare, technologieneutrale Identitätssicherung und eine ab diesem Punkt verschlüsselte Datenspeicherung und -übertragung sichergestellt werden.

VII. Quellen

[1] Vgl. zum erfolgreichen Hack eines Jeeps in den USA (http://www.faz.net/aktuell/feuilleton/medien/wie-zwei-hacker-vom-sofa-aus-einen-jeep-uebernehmen-13715966.html) und der Manipulation eines Narkosegerätes (http://www.spiegel.de/netzwelt/netzpolitik/hacker-manipuliert-narkosegeraet-a-1047258.htm).
[2] Identität bedeutet in diesem Zusammenhang die Summe derjenigen Merkmale, anhand derer ein Individuum oder eine andere im Netzwerk agierende Entität (z.B. ein Gerät oder ein Sensor) eindeutig von anderen unterschieden werden kann. Identitätsmanagement ist die Summe aller Maßnahmen, die notwendig sind, um Identitäten in IT-Systemen eindeutig zu erkennen sowie ihnen genau jene Zugriffe zu ermöglichen, die sie aktuell im Rahmen ihrer Tätigkeit benötigen
[3]Studie „*Internet of Things – Hype oder Motor für den deutschen Mittelstand?*“, Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt, Dezember 2014.
4 Meldung bei Spiegel Online, abrufbar unter http://www.spiegel.de/netzwelt/netzpolitik/hacker-manipuliert-narkosegeraet-a-1047258.html.
5 Meldung bei ebdgadget.de, abrufbar unter http://de.engadget.com/2015/08/02/infusionspumpen-hack-us-behorde-warnt-krankenhauser/.
6 Meldung bei derStandard.at, abrufbar unter http://derstandard.at/2000020752533/Lampen-Schloesser-Wiener-fanden-Schwachstelle-in-ZigBee.
7 Meldung bei Handelsblatt, abrufbar unter http://www.handelsblatt.com/technik/it-internet/auto-per-handy-ferngesteuert-hacker-schalten-corvette-bremsen-ab/12180170.html.
[8] Bundesdatenschutzgesetz, Telemediengesetz und weitere sektorspezifische deutsche Gesetze aber auch die derzeit noch geltende EU-Datenschutzrichtlinie 1995/46/EG wie auch die geplante EU-Datenschutz-Grundverordnung.
[9] Hervorzuheben sind das IT-Sicherheitsgesetz und die gerade in der Entstehung befindliche NIS-Richtlinie auf EU-Ebene.
[10] Vgl. die Meldung bei Heise, http://www.heise.de/security/meldung/Cisco-warnt-vor-Attacken-mittels-manipulierter-Firmware-2778535.html.
[11] Vgl. auch BMWi, Entwurf zur Messsystemverordnung, S. 2.
[12] Richtlinie 2012/27/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2012.
[13] Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz - EnWG).
[14] Vgl. BMWi, Entwurf zur Messsystemverordnung, S. 22 f.
[15] Vgl. BMWi, ebda., S. 25.
[16] Vgl. BMWi, ebda., S. 22.
[17] Vgl. BMWi, ebda., S. 26.
[18] Vgl. BMWi, ebda., S. 26.
[19] Art. 79 des Kommissionsentwurfs der Datenschutz-Grundverordnung.
[20] Vgl. die Pressemitteilungen des VZBV zu erfolgreichen Klagen gegenüber Google (http://www.vzbv.de/pressemitteilung/vzbv-gewinnt-klage-gegen-google) und gegenüber Samsung (http://www.vzbv.de/pressemitteilung/samsung-app-store-zahlreiche-klauseln-rechtswidrig).
[21] Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts, BT-Drs 18/4631.
[22] Art. 76 Abs. 2 des Ratsentwurfs der DS-GVO.
[23] In den USA ist es Hackern jüngst gelungen, über Schwachstellen in der Unterhaltungselektronik auf die Steuerung und auch die Bremsen eines Jeeps zuzugreifen und diesen, ohne Eingriffsmöglichkeit des Fahrers, zum Stillstand zu bringen, vgl. Meldung bei Faz.net, abrufbar unter http://www.faz.net/aktuell/feuilleton/medien/wie-zwei-hacker-vom-sofa-aus-einen-jeep-uebernehmen-13715966.html.
[24] Vgl. BMWi, Entwurf zur Messsystemverordnung, S. 17.