PROMOTORENBERICHT
ZUM ZUKUNFTSPROJEKT SICHERE IDENTITÄTEN

Forschungsunion

Wirtschaft und Wissenschaft
begleiten die Hightech-Strategie

Impressum

Herausgeber
Promotorengruppe Sicherheit der Forschungsunion Wirtschaft-Wissenschaft
Dr. Carsten Ottenberg, Giesecke & Devrient
Susanne Kunschert, Pilz GmbH & CO.KG
Prof. Dr. August-Wilhelm Scheer, IMC AG

Redaktion
Fabian Bahr, Giesecke & Devrient
Michael Barth, BITKOM e.V.
Hansjörg Sperling-Wohlgemuth, Pilz GmbH & Co.KG.
Dr. Anne-Sophie Tombeil, Fraunhofer IAO

Layout, Satz, Illustration
SpiegelGrafik, Stuttgart

Kontakt
Fraunhofer IAO, Dr. Anne-Sophie Tombeil
Telefon 0711 970-2146
Anne-Sophie.Tombeil@iao.fraunhofer.de

Auslieferung und Vertrieb
Büro der Forschungsunion im Stifterverband für die Deutsche Wissenschaft e. V.
Oranienburger Str. 13 - 14, 10178 Berlin
bueroderforschungsunion@stifterverband.de

Im Internet unter www.forschungsunion.de

Erscheinungstermin: Juli 2011

© Copyright liegt bei dem Herausgeber. Alle Rechte vorbehalten. Dieses Werk ist einschließlich seiner Teile urheberrechtlich geschützt. Jede Verwertung, die über die engen Grenzen des Urheberrechtsgesetzes hinausgeht, ist ohne schriftliche Zustimmung des Herausgebers unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen sowie die Speicherung in elektronischen Systemen.Für die Richtigkeit der Herstellerangaben wird keine Gewähr übernommen.

PROMOTORENBERICHT
ZUM ZUKUNFTSPROJEKT SICHERE IDENTITÄTEN

Forschungsunion

Wirtschaft und Wissenschaft
begleiten die Hightech-Strategie

Inhalt

1 ZUSAMMENFASSUNG 6

2 SICHERHEIT IN DER HIGHTECH-STRATEGIE 8

2.1 Vorbemerkungen 8

2.2 ITK – zentraler Pfeiler im Bereich Sicherheit 9

3 ZUKUNFTSPROJEKT SICHERE IDENTITÄTEN 15

3.1 Abgrenzung des Themenfeldes 15

3.2 Identitäten und Sicherheit 20

3.3 Handlungsfeld Datenschutz 22

3.3.1 Ausgangslage 22

3.3.2 Themen 23

3.3.2.1 Individualisierung von Identitäten 24

3.3.2.2 Nutzerdatenintensive Anwendungen 27

3.3.2.3 Privacy-enhancing Technologies (PET) 28

3.3.2.4 Datenschutzrecht 31

3.3.3 Handlungsempfehlungen 33

3.4 Handlungsfeld Datensicherheit 35

3.4.1 Ausgangslage 35

3.4.2 Themen 37

3.4.3 Handlungsempfehlungen 39

4 ZUKUNFTSINITIATIVEN 44

4.1 Zukunftsinitiative Sicheres Cloud Computing 44

4.1.1 Ausgangslage 44

4.1.2 Übergreifende Handlungsempfehlungen 45

4.1.2.1 Forschung und Entwicklung 45

4.1.2.2 Regulierung 47

4.1.2.3 Vermarktung 47

4.2 Zukunftsinitiative Sichere Embedded Systems 48

4.2.1 Ausgangslage 48

4.2.2 Kompetenzen und Handlungsbedarf 49

4.2.3 Übergreifende Handlungsempfehlungen 51

5 ROADMAP 55

6 DANKSAGUNG 56

7 PROMOTORENGRUPPE SICHERHEIT 59

Abkürzungsverzeichnis

COTS	Commercial off the shelf
CPS	Cyber-Physical Systems
CRM	Customer Relationship Management
CSRF	Cross-Site Request Forgery
ERP	Enterprise Resource Planning
ES	Embedded Systems
EV-Zertifikate	Extended-Validation-Zertifikate
HTML	Hyper-Text Markup Language
ICANN	Internet Corporation for Assigned Names and Numbers
IGF	Internet Governance Forum
IPv6	Internet Protocol Version 6
ITK	Informations- und Kommunikationstechnologien
M2M	Machine-to-Machine
OWASP	Open Web Application Security Project
PET	Privacy-enhancing Technologies
RFID	Radio Frequency Identification
RL	Richtlinie
SaaS	Software-as-a-Service
SCM	Supply Chain Management
SOA	Service-oriented Architecture
SSL	Secure Sockets Layer
TAN	Transaktionsnummer
XHTML	Extensible Hyper-Text Markup Language

Abbildungsverzeichnis

Abbildung 1: Rolle der Informations- und Kommunikationstechnologien 10
Abbildung 2: Informations- und Kommunikationstechnologien als querschnittlicher Innovationsfaktor (eigene Darstellung) 12
Abbildung 3: Untersuchungsgegenstand 14
Abbildung 4: Identitätsfreigaben und Transaktionswert im Verhältnis 16
Abbildung 5: Geschäftsmodellentwicklung im virtuellen Raum (eigene Darstellung) 17
Abbildung 6: Identitätsfreigaben und Transaktionswert im virtuellen Raum 19
Abbildung 7: Die Top-10 der Online-Communities (Quelle: BITKOM) 22
Abbildung 8: Jeder zweite Internet-Nutzer hat ein Online-Profil (Quelle: BITKOM) 23
Abbildung 9: Infos, Communities und Multimedia (Quelle: BITKOM) 24
Abbildung 10: Internetnutzer begreifen das Web als Gewinn (Quelle: BITKOM) 24
Abbildung 11: Verzicht auf Aktivitäten im Internet – nach Alter (Quelle: BITKOM) 25
Abbildung 12: Security-Usability-Kompromiss (Annahme: Safety konstant) 33
Abbildung 13: Rechnen mit der Wolke (Quelle: BITKOM) 44
Abbildung 14: Embedded Systems in der ITK, Beispiel Smart Factory / Automatisierungspyramide 48

1 ZUSAMMENFASSUNG

Die sichere Identifizierung von Personen und Objekten in der realen und der virtuellen Welt ist unabdingbar für den Schutz unserer offenen Gesellschaft und ihrer freiheitlich-demokratischen Grundordnung. Sichere Identitäten sind zentrales Element für die Freiheit des Einzelnen und für die Schaffung einer gesellschaftlichen Vertrauenskultur.

Identitäten sind mit der Fortentwicklung der Informations- und Kommunikationstechnologien (ITK) einem begrifflichen Wandel unterworfen. Dieser wird durch die Virtualisierung von Identitäten in Netzen, insbesondere dem World Wide Web, getragen. Identitäten müssen geschützt werden, denn mit steigender Werthaltigkeit der über das Netz übertragenen, dorthin ausgelagerten oder dort verarbeiteten Daten steigt der Anreiz, Angriffe zu unternehmen oder Netze zu stören. Die Promotorengruppe Sicherheit der 17. Legislaturperiode konzentriert ihre Arbeit daher auf das Zukunftsprojekt »**Sichere Identitäten**«.

Für Nutzer, Anbieter, Wissenschaft und Forschung sowie die Politik ergeben sich zwei große Handlungsfelder: Datenschutz und Datensicherheit. Entsprechende **Handlungsempfehlungen** umfassen:

- **Datenschutz.** Herstellung von Transparenz beim Nutzer hinsichtlich der Verarbeitung, Weitergabe, des Verwendungszwecks seiner Daten und etwaiger Risiken. Stärkung der Eigenverantwortung des Nutzers einschließlich durchsetzbarer Nutzerrechte bei der Änderung von Identitäten im Netz. Proaktiveres Vorgehen bei der internationalen Vermarktung deutscher Datenschutzregulierungen als Wettbewerbsvorteil. Weiterentwicklung des deutschen Datenschutzrechts hin zu einem technologie- und nutzeradäquaten Informationsschutzrecht. Initiativen zur Entfaltung der Möglichkeiten sicherer, ITK-gestützter Mechanismen zur Stärkung der partizipativen Demokratie.
- **Datensicherheit.** Definition nationaler Kernfähigkeiten der IT-Sicherheit einschließlich des Ausbaus der deutschen Systemkompetenz im Bereich der Kryptologie. Aufbau einer Sicherheitsökonometrie. Untersuchung potentieller Schwachpunkte im Internet. Ausbau der deutschen Beratungs- und Evaluierungskompetenz im Bereich der Hardware- und Softwaresicherheit. Verstärkung der zwischenstaatlichen Zusammenarbeit zur Sicherheit in Netzen. Formulierung einer deutschen Technologieaußenpolitik.

Die vorstehenden Handlungsfelder tragen ferner dazu bei, generationen- und lebensumfeldübergreifend gleichwertige Zugangsbedingungen zu Netzdiensten bereitzustellen. Dadurch wird die Teilhabe an der netzbasierten Wissensgesellschaft erleichtert. Sichere Identitäten haben somit auch eine gesellschaftliche Dimension, die ethische Grundfragen berührt.

Der Bericht verdeutlicht, dass sichere Identitäten stets kontext- und anwendungsbezogen zu definieren sind. Sicherheit kann nur in einem ordnungspolitischen Rahmen existieren, der den grenzenlosen Charakter des Internets berücksichtigt. Sicherheit ist im virtuellen Raum nicht statisch-absolut. Sie ist ein im Zusammenspiel von technischen Lösungen, politisch-regulativen Eingriffen und Verhaltens lenkenden Maßnahmen anzustrebendes Ziel.

Sicherheit als Querschnittsthema muss zudem stärker auf die Bedürfnisse der Anwender eingehen. Tragfähige Geschäftsmodelle werden daher auch die Quantifizierbarkeit der Effektivität und Effizienz von Sicherheitslösungen berücksichtigen müssen,

um die in Deutschland erzielten exzellenten Forschungsergebnisse international noch besser vermarkten zu können.

Am Beispiel der beiden Zukunftsinitiativen **»Sicheres Cloud Computing«** und »**Sichere Embedded Systems«** werden diese Herausforderungen des Themenfelds der sicheren Identitäten illustriert und Handlungspfade aufgezeigt.

Im **Cloud Computing** ist in den kommenden Jahren mit einem enormen Marktwachstum zu rechnen. Die Entfaltung der Cloud-Potenziale für deutsche Anbieter im Software- und Service-Bereich wird dann gelingen, wenn die Sicherheit der ausgelagerten Daten und neuartigen Dienste auf die Bedürfnisse des Anwenders fokussiert werden kann. Die Handlungsempfehlungen der Promotorengruppe umfassen die folgenden Elemente:

- F&E-Aktivitäten zur rollen- und ebenengerechten Datenverschlüsselung auf Feld- und Datensatzebene. Schaffung eines Third-Party-Mehrwertanwendungs-Layers mit den Dimensionen Sicherheit und Compliance. Realisierung eines Exzellenzzentrums Sicherheitsökonometrie für die Mess- und Bewertbarkeit von Sicherheitsniveaus und Restrisiken. Für die genannten Bereiche ist die Einbeziehung des Anwenders erfolgskritisch.
- Schaffung eines nationalen Testbeds »Sicheres Cloud Computing« zur Überprüfung der Leistungsfähigkeit und Robustheit von sicheren Cloud-Architekturen und –Diensten.
- Konzeption eines Siegels für nationale sichere Anbieter als Teil einer Vermarktungsinitiative.

Die Sicherheit von **Embedded Systems** wird in den kommenden Jahren zu einer Bewährungsprobe beim Schutz kritischer Infrastrukturen. Die Bereiche, in denen Embedded Systems wirken, reichen dabei vom Maschinen- und Anlagenbau bis zum selbstbestimmten Leben im Alter. Die Promotorengruppe Sicherheit geht davon aus, dass die Embedded-Systems-Märkte der Zukunft von einer am gesamten Wertschöpfungsprozess orientierten Lösungslogik beherrscht werden und formuliert folgende Handlungsempfehlungen:

- Ausbau der nationalen systemischen F&E-Kompetenz mit den Schwerpunkten **»security by design«** und **»security economics«**. Dies schließt die Förderung von wissenschaftlichem Nachwuchs mit Systemdesign-Fähigkeiten in einem interdisziplinären Aus- und Weiterbildungsansatz ein.
- Untersuchungen zur Identifikation sicherheitsrelevanter ES-Anwendungsfelder auf nationaler (sowie europäischer, internationaler) Ebene und zu Lösungen für die Integration von Embedded Systems in Prozessketten mit sicherer gegenseitiger Identifizierung, Authentifizierung und Validierung.
- Initiativen zur Förderung der Einflussnahme deutscher Institutionen auf die Setzung internationaler Normen und Standards.
- Vorantreiben des Akzeptanzmanagements für Sicherheitslösungen. Dazu zählen die Vereinheitlichung der Begriffsbasis, die Definition von Schutzzielen sowie die Festlegung von Mindestanforderungen für deren Sicherheit.
- Schaffung eines Demonstrators für sichere, interoperable Embedded Systems als gemeinsame Aktivität einer Anwenderbranche mit Forschungseinrichtungen und der ITK-Industrie im Rahmen eines ausgewählten Cyber-Physical-Systems-Szenarios.

2 SICHERHEIT IN DER HIGHTECH-STRATEGIE

2.1 Vorbemerkungen

Als Teil der Hightech-Strategie nimmt das Themenfeld Sicherheit in zweierlei Hinsicht eine besondere Rolle ein. Es ist ein international im Wachstum befindliches, allerdings nur schwer abgrenzbares Forschungs- und Geschäftsfeld. Andererseits stellt es eine querschnittlich wirkende Unterstützungsfunktion für weitere Themenfelder dar.

Darauf wurde bereits in der vorherigen Forschungsunion aufmerksam gemacht; zudem wurden sechs Handlungsfelder definiert:

- **»Die Zukunft mitbestimmen«** – mit dem Schwerpunkt der aktiven Interessenvertretung Deutschlands sowohl im europäischen Sicherheitsforschungsprogramm als auch bei der Gestaltung des europäischen Marktes für Sicherheitsprodukte und –standards. Diese Forderung ist nach wie vor richtig und wird von den Promotoren nachdrücklich unterstützt. Insbesondere das vielzitierte Level Playing-Field im Bereich der nichtmilitärischen Sicherheitsprodukte ist bei weitem nicht erreicht, wenngleich legislativ mit der Verabschiedung des sog. Defence Package ein Schritt in die richtige Richtung unternommen wurde. Es kommt nunmehr darauf an, die Rechtstexte so umzusetzen, dass in der unternehmerischen Praxis nicht einseitig Wettbewerbsvorteile der deutschen Industrie aufgegeben werden, ohne eine vergleichbare Öffnung der nach wie vor national fragmentierten, oft protektionistisch verschlossenen Sicherheitsmärkte unserer europäischen Partner politisch zu forcieren.
- **»Den Markt aktiv gestalten und erschließen«** – hierbei begrüßt die Promotorengruppe Sicherheit die Ausgestaltung des nationalen Sicherheitsforschungsprogramms. Die Einbeziehung interessierter Akteure in den Agendasetzungsprozess gewährleistet eine anwendungsnahe Ausrichtung des Programms zur Stärkung der vorhandenen Kompetenzen am Standort Deutschland. Gleichzeitig können inhaltliche Synergien mit dem europäischen Forschungsrahmenprogramm erschlossen werden.

- **»Szenarienorientierte Ansätze weiter verfolgen«** – in ihren Aktivitäten nimmt die Promotorengruppe Sicherheit die Empfehlung der vorhergehenden Forschungsunion auf. Sie benennt nachstehend die aus ihrer Sicht vordringlich zu bearbeitenden Handlungsfelder.
- **»Vernetzung aller Partner anstreben«** – dieses Teilziel ist permanent zu verfolgen, ohne dabei die thematischen Prioritäten aus dem Blickwinkel zu verlieren.
- **»Technologiefelder miteinander verbinden«** – die Promotorengruppe Sicherheit versteht diese Empfehlung als Leitbild ihres Handelns, Sicherheit nicht nur als eigenständiges Forschungs- und Geschäftsfeld, sondern auch als querschnittlich zu betrachtendes Themenfeld der Bedarfsfelder Klima und Energie, Mobilität, Kommunikation und Gesundheit zu verfolgen.
- **»Standards mitprägen«** – die Promotorengruppe sieht nach wie vor Handlungsbedarf mit einem besonderen Fokus auf die Bedürfnisse des industriellen Mittelstands, um diese in das von neuen globalen Wettbewerbern geprägte Umfeld nachhaltig einzubringen.

2.2 ITK – zentraler Pfeiler im Bereich Sicherheit

Mit der seit rund 25 Jahren andauernden Durchdringung gesamtwirtschaftlicher Wertschöpfungsketten durch Informations- und Kommunikationstechnologien ist ein grundlegender Paradigmenwechsel zu verzeichnen. Dieser umfasst die Entwicklung vom Einsatz als Unterstützungswerkzeug in unternehmensinternen Sekundärprozessen über die Penetration von Produktionsprozessen bis hin zur Schaffung neuartiger, netzbasierter Geschäftsmodelle. Parallel findet eine mit der technologischen Entwicklung verschränkte und sich gegenseitig verstärkende Transformation des industriellen und des Lebensumfelds statt. Eine zentrale Herausforderung ist die dramatische Verkürzung von Innovationszyklen und damit verbunden die Notwendigkeit flexibler Reaktion. Einige Beispiele zur Illustration:

- Fertigungsstrukturen und Wertschöpfungsketten werden global (deutlich sichtbar zum Beispiel beim Thema integrierte Schaltkreise). Sie folgen damit der kurzzyklischen Anwendernachfrage nach immer leistungsfähigerer Technologie. Mit der Verminderung der Fertigungstiefe in Deutschland und der damit einhergehenden Ausweitung von Wertschöpfungsnetzen wird auch die Kontrolle über die Integrität der zugelieferten Vor- und Zwischenprodukte dezentralisiert. Somit sind technisch vielfältigere Angriffsmöglichkeiten potentiell denkbar. Sie werden mit der technologischen Komplexitätsausweitung weniger kontrollierbar und können bei sicherheitsrelevanten Anwendungen ein Risiko darstellen.
- Die Vision der »atmenden Fabrik« wird Wirklichkeit. Automatisierungs- und Produktionsumstellungen werden zu Effizienzgewinnen führen. Unter dem Blickwinkel der globalen Produktionsstandort-Vernetzung ist IT-Sicherheit in industriellen Fertigungsprozessen, der Fernwartung usw. bereits architektonisch-konzeptionell zu berücksichtigen.
- Mobiles Bezahlen (Mobile Payment) führt in einigen Staaten dazu, dass die bisherigen Telekommunikationsanbieter – vorwiegend im Bereich der Infrastruktur-Dienstleistungen aktiv – plötzlich einen Teil der Rolle wahrnehmen, die bisher Geschäftsbanken als Dienstleister rund um den Zahlungsverkehr vorbehalten war.
- Die Auslagerung von Daten in die Cloud schafft neue Teilnehmer in der Wertschöpfungskette. Gleichermaßen werden seit langem bekannte Paradigmen (zum Beispiel die Umstellung von »Besitz« auf »Zugang«) nun auf die Wissensgesellschaft ausgeweitet. Dies bringt neue Herausforderungen an die Sicherheit mit sich.
- Die durchgehende informationstechnische Vernetzung unserer Gesellschaft und die damit verbundenen IT-Sicherheitslücken machen Bürger und Organisationen nicht nur zum Ziel von Sicherheitsangriffen, sondern (Beispiel Bot-Netze) auch zur (unwissentlichen) Schwachstelle.

Informations- und Kommunikationstechnologien sind in diesem Kontext nicht mehr nur unterstützende Technologien, sondern Treiber der volkswirtschaftlichen Produktivitätssteigerung. Sie begleiten Wandlungsprozesse einst abgeschotteter Staaten und Systeme auf dem Weg zur politischen Stabilität und Demokratisierung, wie die seit Beginn der 1990er Jahre andauernden weltpolitischen Umwälzungen eindrucksvoll untermauern.

ITK sind ein wesentliches Element unserer Lebensqualität, Instrument der sozialen Interaktion und immer häufiger konstitutiver Teil des privaten und beruflichen Umfelds. Sie tragen zur Transparenz, Nachvollziehbarkeit und Effizienz des Verwaltungshandelns bei (»open government«) und sind ein zentraler Pfeiler für die Möglichkeiten zur demokratischen Teilhabe.

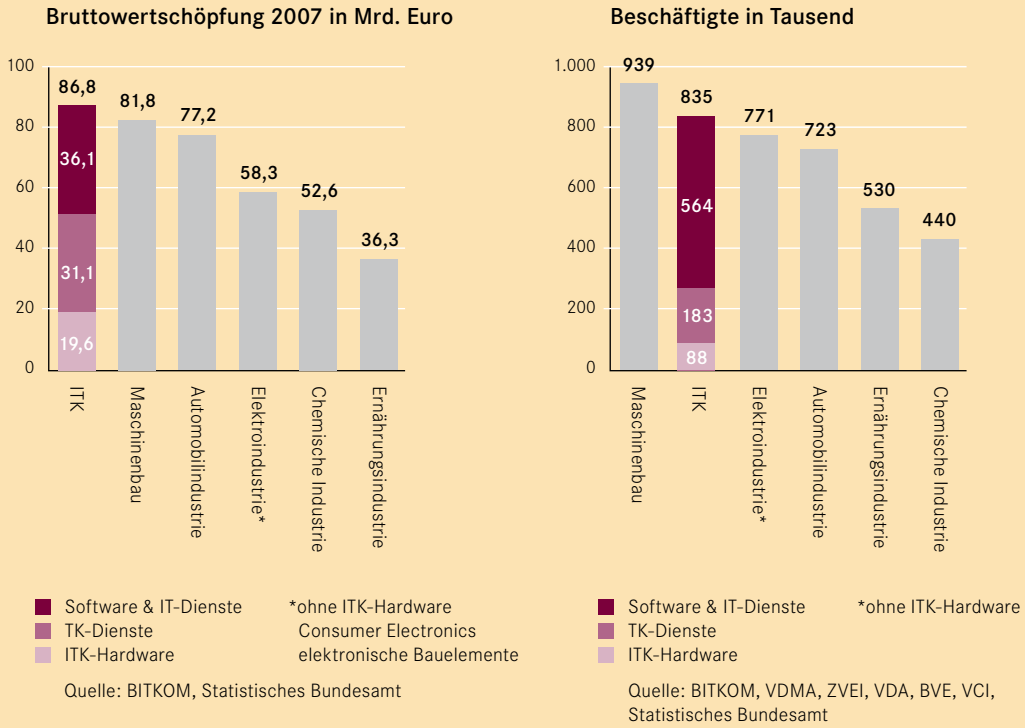


Abbildung 1: Rolle der Informations- und Kommunikationstechnologien

Mit dem Eintritt in die international vernetzte, interdependente Wissensgesellschaft wird es notwendig, die vielmals in technologischen Innovationssprüngen (und nicht in einem vielleicht wünschenswerteren spiral development) auftretenden unerwünschten Nebeneffekte der Vernetzung zu identifizieren und Handlungsspielräume zu deren Begrenzung aufzuzeigen. Dabei spielen sichere **Identitäten** eine herausragende Rolle: Als virtuelle Spiegelbilder des Bürgers im Netz wie auch als objektgebundene Merkmale in industriellen Prozessen.

Die sichere Identifizierung (je nach Kontext auch Pseudonymisierung und Anonymisierung) von Personen und Objekten ist unabdingbar für den Schutz unserer offenen Gesellschaft und für die Verteidigung unserer freiheitlich-demokratischen Grundordnung. Sichere Identitäten sind der Baustein für die Freiheit des Einzelnen: Als Bürger, als Verbraucher, als Inhaber intellektuellen Eigentums. Die Promotorengruppe Sicherheit konzentriert ihre Arbeiten daher bewusst auf die Themenfelder Datenschutz und Datensicherheit.

Der aktuelle gesellschaftspolitische Diskurs zu Fragen der Sicherheit von Daten und Identitäten spiegelt ein breites Meinungsspektrum der Akteure wider. International – vgl. beispielsweise die transatlantischen Debatten auf dem Gebiet des Datenschutzes – wird zudem die Spannbreite kulturell und mentalitätsbedingter Unterschiede in Bezug auf Sicherheit deutlich: Sei es bei der Stärke der Ausprägung von als notwendig erachteten Sicherheitsmechanismen, sei es bei der Einschätzung von Bedrohungsszenarien, sei es hinsichtlich unterschiedlicher und sicherheitsökonometrisch schwer erfassbarer Risikoakzeptanzschwellen.

Eine oft wahrzunehmende Grundkonstante der öffentlichen Diskussion in Deutschland im Zusammenhang mit ITK-Angeboten, in denen die Sicherheit des Nutzers wichtig ist, stellt die nach anfänglichem Enthusiasmus der Öffentlichkeit rasch einsetzende Skepsis dar. Aus Sicht der Promotorengruppe wäre es jedoch eine intellektuelle Verkürzung, diese Skepsis pauschal als Technikfeindlichkeit einzuordnen. Vielmehr drückt sich darin das berechtigte Anliegen der Nutzer aus, innovative ITK-Lösungen nutzen zu können, ohne Kompromisse in Fragen des Datenschutzes und der Datensicherheit eingehen zu müssen. Die Funktionsfähigkeit vertrauenswürdiger Technologien (nachgewiesen beispielsweise durch deren erfolgreiche Akkreditierung, Zertifizierung etc.) und die Erreichung der als schutzwürdig erachteten (politischen, juristischen) und mit verhältnismäßigem Mitteleinsatz realisierbaren Sicherheitsstufen bedingen dabei einander.

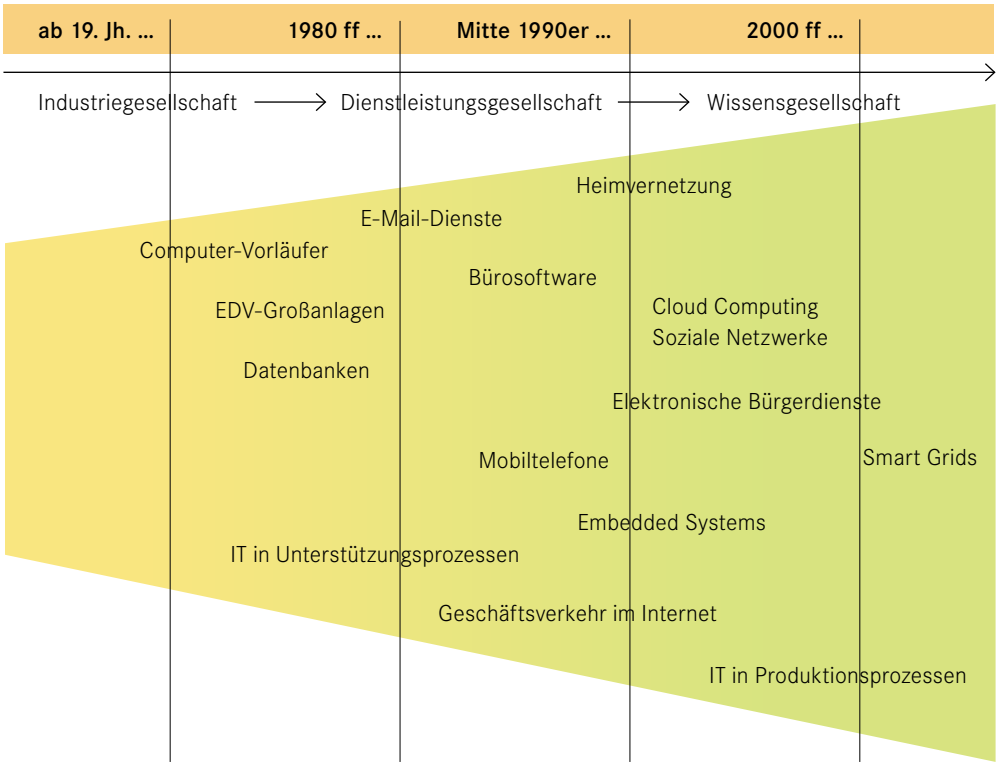


Abbildung 2: Informations- und Kommunikationstechnologien als querschnittlicher Innovationsfaktor (eigene Darstellung)

Einzelfälle auftretender Sicherheitslücken führen seitens des Regulators häufig zu Ad-hoc-Reaktionen (medial, legislativ). Diese laufen notwendigerweise Gefahr, mit dem technologischen Fortschritt (oder der bei der Erbringung grenzüberschreitender Leistungen begrenzten nationalen Regulierungshoheit) nicht Schritt halten zu können. Umso wichtiger ist es, bereits vorgelagert die Sicherung von Identitäten zu betrachten und Möglichkeiten zu finden, wie Deutschland als das führende europäische Hochtechnologieland

- **seine Bürger schützen kann – ohne sie bei der Nutzung netzbezogener Dienste zu bevormunden –**
- **seine technologische Spitzenrolle in der netzbasierten Wissensökonomie halten und ausbauen kann – ohne sich abzuschotten –**
- **seine exzellenten Universitäts-, Hochschul- und Forschungseinrichtungen international vernetzen kann – ohne unkontrollierten Wissenstransfer durch ungesicherte Netze zu riskieren.**

Die Promotorengruppe Sicherheit ist sich des hohen Anspruchs und der Verantwortung bewusst, die mit der Behandlung des Themenfelds sichere Identitäten verbunden sind. Sichere Identitäten stellen einen bestimmten Ausschnitt der Sicherheitsforschung dar. Sie sind Treiber der Entwicklung im Bereich ITK-Sicherheit, wirken unterstützend bei der zivilen Sicherheitsforschung und schaffen übergreifend Mehrwert im Sinne von Sicherheitsgewinn. Handlungsempfehlungen, ja bereits die Benennung von Handlungsfeldern, sind sozialisationsgebunden, kulturell konditioniert und wertegeleitet. Demokratische Grundwerte der westlichen Gesellschaften werden als handlungsbestimmende Maxime des verantwortlichen Umgangs mit Daten angesehen.

Die Auswahl der betrachteten Handlungsfelder ist insofern willkürlich, als Sicherheit eine natürliche Querschnittsfunktion in Anwendungen vielfältiger Natur ist: Von Cloud Computing zu Smart Grids, von industriellen Automationsprozessen bis zum Schutz von Firmennetzen. Die gewählten Handlungsfelder umfassen die Schnittmenge von IT-Sicherheit, ziviler Sicherheit bis hin zu funktionaler Sicherheit (in Teilen). Treibende Frage in den Überlegungen der Promotorengruppe ist daher die folgende: Kann Sicherheit als Ausgangspunkt für die Erarbeitung neuer Geschäftsmodelle genutzt werden?

Die Promotorengruppe Sicherheit hat ihre Handlungsempfehlungen mit den Ergebnissen dreier Expertenworkshops verglichen, die im Februar 2011 durchgeführt wurden. Die Zusammensetzung der Expertengruppen entsprach dem Wunsch der Promotorengruppe, die bereits im ersten Bericht der Promotorengruppe als wesentlich erachteten Elemente a priori von der Anwenderseite untersuchen zu lassen, mit deren Erfahrungen zu spiegeln, auf inhaltliche Konsistenz zu prüfen und abzugleichen sowie anschließend Handlungsempfehlungen zu erarbeiten. Diese Elemente umfassen:

- Regulatorisches Umfeld im nationalen und internationalen Kontext;
- Technologische Leistungsfähigkeit der deutschen (Sicherheits-)Wirtschaft;
- Fokussierung des Forschungs- und Bildungsumfelds;
- Umsetzungskompetenz in tragfähige Geschäftsmodelle über die Produkteinführung hinaus;
- Absorptionsfähigkeit neuer technologischer Lösungen durch in Deutschland verortete Anwenderindustrien;
- Akzeptanz neuer technologischer Anwendungen durch die Nutzer;

- Gesellschaftliche Akzeptanz der notwendigen sicherheitsorientierten Rahmenbedingungen

Daraus ergeben sich drei Handlungsfelder, die sich bereits im ersten Bericht der Promotorengruppe Sicherheit als relevant abzeichneten:
- Technologische Aspekte;
- Politik und Regulierung;
- Nationale und internationale Aspekte der Vermarktung.

Dabei wurden Hemmnisse und Fähigkeitslücken benannt, Empfehlungen ausgesprochen und einzelnen Akteuren bzw. Akteursgruppen zugeordnet.

Der nachstehende Folgebericht der Promotorengruppe Sicherheit kann keine allumfassende Bestandsaufnahme der mit sicheren Identitäten einhergehenden Herausforderungen sein, sondern konzentriert sich auf ausgewählte Handlungsfelder. Der Bericht erhebt gleichwohl den Anspruch, zentrale gesellschaftliche Diskussionen aufzugreifen und einzuordnen und darauf aufbauend technologie- und innovationspolitische Handlungsempfehlungen abzuleiten.

Unter Inkaufnahme teilweiser struktureller Überschneidungen befasst sich der vorliegende Bericht mit dem **»Zukunftsprojekt Sichere Identitäten«**. Als Anwendungsfälle werden exemplarisch die **Zukunftsinitiativen »Sichere Cloud«** und **»Sichere Embedded Systems«** vorgestellt.

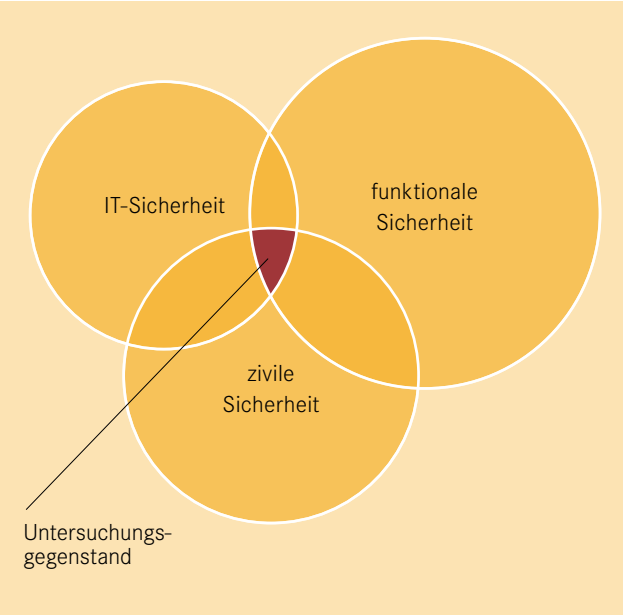


Abbildung 3: Untersuchungsgegenstand

3 ZUKUNFTSPROJEKT SICHERE IDENTITÄTEN

3.1 Abgrenzung des Themenfeldes

Die sichere Zuordnung von Identitäten ist die Voraussetzung für Transaktionen aller Art. Vom »Geschäft per Handschlag« bis zur Bestellung per Mausklick: Identitäten schaffen Vertrauen. Konventionell lassen sich Identitäten leicht anhand weniger Merkmale definieren. Im virtuellen Raum, insbesondere im Internet, wird dies mangels visuellen Kontakts schwieriger. Es ist daher eine anspruchsvolle Aufgabe, in der Komplexität von Netzen Identitäten eindeutig zuzuordnen und damit die Transaktionssicherheit zu schaffen, die im realen Leben leicht zu schaffen ist. Hier setzen die Arbeiten der Promotorengruppe Sicherheit an.

Bei der Abgrenzung des Themenfeldes sind zwei Fälle zu unterscheiden.

1. **Objektorientierte Identitäten.** Darunter fallen zum Beispiel das Internet of Things (im Kontext der RFID-Nutzung) bis hin zur Robotik oder zum futuristischen Smart Dust. Sensoren oder Aktoren in diesen Anwendungskontexten können nur dann sinnvoll eingesetzt werden, wenn ihre Ansprache und Reaktion eindeutig erfolgen kann. Dies schließt Interaktionen auf verschiedenen Abstraktionsebenen (z. B. Einzelobjekt, Palette, Container) oder in unterschiedlichen Gruppen nicht aus.

2. **Personenbezogene und personenbeziehbare Daten.** Abb. 4 illustriert den im Grenzbereich stark steigenden Sicherheitsbedarf bei der Kommunikation persönlicher Daten. Hinzu kommt die Vielzahl von Anwendungen, bei denen zwar unmittelbar keine persönlichen Daten übertragen werden, sich aber beispielsweise aus Art, Häufigkeit und Inhalt der übertragenen Daten hinreichend genau auf eine Person schließen lässt.

Dies sei an einem Beispiel illustriert. Der durchschnittliche Käufer im Supermarkt wird an der Kasse seinen Einkauf mit Bargeld bezahlen, sofern es sich um kleinere Beträge handelt. Persönliche Daten werden dabei nicht von ihm verlangt. Geht es um mittlere Summen, wird er den Betrag in Zukunft vielleicht per Handy (NFC), derzeit überwiegend noch mit Debit-Karte, begleichen. Im letzten Fall werden bestimmte Daten – Kontonummer, Name, Einverständniserklärung zur Lastschrift bzw. PIN-Nummer etc. – von ihm verlangt. Handelt es sich um größere Beträge, die vielleicht noch im Ausland bezahlt werden, steigt das Sicherheitsbedürfnis des Nutzers – er wird mit seiner Kreditkarte bezahlen. Vielleicht nutzt er gleichzeitig seine Kreditkarte in einem Bonusprogramm: Dann wird er umso häufiger bereit sein, sein Kaufverhalten elektronisch zu dokumentieren, um Vorteile zu erlangen. Somit gibt er zunehmend Daten von und über sich – und damit einen Teil seines Verhaltens, seiner Identität, preis. Allerdings werden in diesem einfachen Beispiel nur wenig Informationen über Anwendungsgrenzen und –kontexte hinweg übermittelt: Den Betreiber des Supermarkts interessiert wahrscheinlich nur das Einkaufsverhalten in seinem Markt, den Anbieter des Bonusprogramms die Auswahl der Einkaufsorte usw.

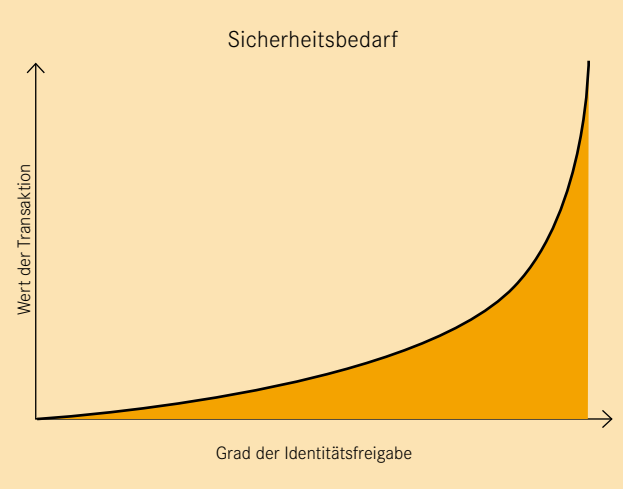


Abbildung 4: Identitätsfreigaben und Transaktionswert im Verhältnis

Für die weitere Betrachtung ist insofern die Feststellung wesentlich, dass es die eine Identität nicht gibt. Es ist stets nach Betrachtungsebene und Betrachtungsgegenstand (Anwendung) zu differenzieren.

In der realen Welt bilden »physische« Identitäten (zum Beispiel bestimmte Klassen biometrischer Merkmale) den Ausgangspunkt der Betrachtung. Sie sind durch in der Regel unabänderliche Teilelemente charakterisiert. Diese sind unabhängig mess- und validierbar.

Im virtuellen Raum ist der Begriff der Identität unscharf. Die Kommunikation persönlicher Daten ist weitestgehend vom Nutzer gesteuert und bestimmt. Sie bemisst sich nach den jeweiligen Anwendungen. Die Art und der Umfang der persönlichen Daten variieren dabei ganz erheblich: Von der Lieferadresse und den Rechnungsdaten bei Internet-Einkäufen bis zur freiwilligen Übermittlung persönlicher Gewohnheiten in sozialen Netzwerken.

Das heißt: Während sich in der realen Welt die übermittelten Identitätsbestandteile und deren Einsatzzweck relativ klar abgrenzen lassen, wird diese klare Zuordnung in der virtuellen Welt schwieriger. Nutzer übermitteln abhängig vom Kontext Daten, die an sich weder Teil einer Identität sind bzw. nur fragmentarischen Wert besitzen. Sie übermitteln ferner durch ihr Verhalten im Netz oft ohne ihr Wissen Daten, welche andere, bruchstückhafte Daten ergänzen, aber für sich genommen nicht auf Identitäten schließen lassen. Erst in der Zusammenführung dieser Elemente können Informationen generiert werden. Damit ergibt sich die Möglichkeit, Rückschlüsse auf Identitäten zu ziehen. Diese stehen dann – begrifflich nur lose gekoppelt – neben dem klassischen Verständnis dessen, was eine Identität ausmacht. Diese

Kontextgebundenheit zeigt: Ein einheitliches Schutzniveau oder eine einheitliche technisch-regulatorische Lösung zur Sicherung von Identitäten im virtuellen Raum wird es nicht geben. Der Trend scheint eher hin zu Lösungen für adäquate, mit unterschiedlichen technischen Schutzvorkehrungen, Vertraulichkeitsstufen bzw. Vertrauensebenen versehene Identitätsniveaus zu gehen.

Damit wird auch deutlich, dass innerhalb des so definierten Themenfeldes dem Nutzer und dem Infrastruktur- und dem Diensteanbieter eine besondere Rolle zukommt: Als Nachfrager, Übermittler, Verarbeiter und Nutzer persönlicher Daten. Identitäten im virtuellen Raum entsprechen damit im Modell den **Schnittpunkten von Angebot und Nachfrage in wettbewerblich organisierten, segmentierten Märkten.**

Dies wird in Abb. 5 für die Entwicklung von Geschäftsmodellen, die auf der Preisgabe persönlicher Daten beruhen, verdeutlicht. Ab dem Punkt, an welchem sich Nutzer und Anbieter auf einen für beide akzeptablen Preis für eine Dienstleistung oder ein Produkt einigen, kommen zunächst Geschäfte zustande. Der Mehrwert, den die Anbieter mit steigenden Informationen zum und über die Nutzer sodann für sich generieren können, übersteigt für eine gewisse Zeit die unmittelbare Nutzernachfrage (orange hinterlegter Bereich). Diese angebotsorientierte Situation hält solange an, wie sich zusätzliches Wissen über die Nutzer in neue Geschäftsmodelle umsetzen lässt.

Zunehmend steigen aber die von den Nutzern zu tragenden Kosten: Sicherheitsrisiken, Datenschutzsensibilisierung usw. Parallel können die Anbieter zwar noch neue Geschäftsmodelle entwickeln, greifen aber dafür zunehmend auf Informationen zurück, die sich aus vorliegenden Nutzerdaten generieren lassen. Dies können beispielsweise Nutzerdaten sein, welche bereits aus

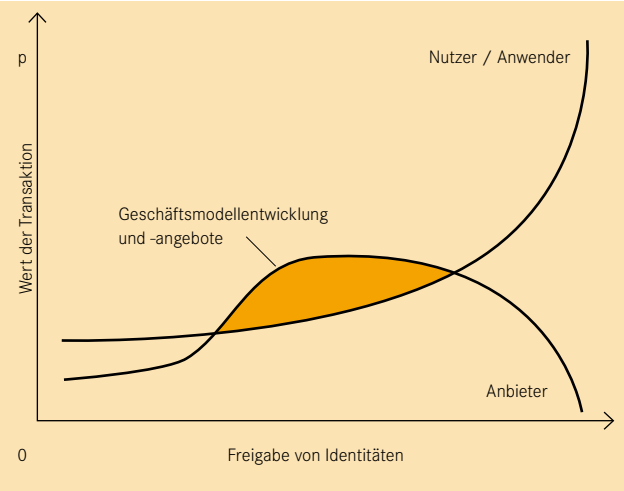


Abbildung 5: Geschäftsmodellentwicklung im virtuellen Raum (eigene Darstellung)

anderen Anwendungen bekannt sind oder beigestellt werden. Somit vermindert sich der Grenznutzen für die Anbieter bei steigenden Kosten für deren Datenhaltung, -übermittlung und -verarbeitung. Ab dem zweiten Schnittpunkt in der Abbildung kämen somit keine neuen Geschäftsmodelle mehr zustande.

Die Rolle der Informations- und Kommunikationstechnologien ist dabei zentral. Sie stellen als befähigende Treiber (Enabler) im virtuellen Raum folgende Verbindungen her:

- Zwischen dem Individuum als Verbraucher und dem Anbieter im elektronischen Geschäftsverkehr (zum Beispiel Versandhandel);
- Zwischen dem Individuum in sozialen Netzwerken als Nachfrager von Kontakten und entsprechenden Anbietern (»Freunden«);
- Zwischen dem Individuum als Bürger (und Nachfrager bestimmter hoheitlicher und damit qua Definition monopolistischer Leistungen) und dem Staat.

Der Umfang der übermittelten virtuellen Identitätsbestandteile, wie oben aufgeführt, variiert in jedem Szenario.

Heruntergebrochen auf die einzelne Identität und den jeweils relevanten Geschäftsprozess stellt sich sodann die Frage der Schutzwürdigkeit, des Schutzbedarfs und der Werthaltigkeit (im o. a. Marktmodell mit Blick auf die Gleichgewichtspreise, Abb. 5) sowohl der physischen als auch virtuellen Identitäten. Daraus kann Handlungsbedarf in den entsprechend unterschiedlichen Rechts-, Regulierungs- und Forschungsfeldern abgeleitet werden.

Wofür »Werthaltigkeit« in diesem Zusammenhang steht, ist heute vom individuellen Nutzer schwer einzuschätzen. Noch vor zehn, fünfzehn Jahren konnte der Nutzer auch elektronischer Dienste – genannt sei das obige Beispiel des Bezahlvorgangs an der Ladenkasse – klar einschätzen, welche Gegenleistung seiner Leistung (der Freigabe seiner Kontodaten, seines Namens usw.) entsprach. Im Idealfall ging ein höherer Wert des Transaktions gutes mit der Preisgabe sensiblerer Identitätsbestandteile einher (vgl. Abb. 4). Dies ist heute durch den Nutzer virtueller Dienste deutlich schwerer einzuschätzen.

Das bisherige zweidimensionale Schema wird mit fortschreitender technologischer Entwicklung ergänzt. Die Erhebung zusätzlicher Informationen zum Nutzerverhalten im zeitlichen Verlauf kommt hinzu (in Abb. 6 als Zeitachse dargestellt). Dazu tragen beispielsweise die innerhalb eines Anwendungskontextes gewonnenen Informationen zum Nutzerverhalten bei: Der Nutzer gibt bestimmte Elemente seines Nutzerverhaltens für mehr Komfort oder andere Gegenleistungen preis. Der Anbieter wiederum kann aus diesen Daten weitere Geschäftsmodelle entwickeln. Über die Zeitachse lässt sich so eine virtuelle Nutzeridentität annähernd umreißen. Sie kann durch die Anreicherung mit weiteren Daten aus anderen Anwendungen heraus ergänzt und analytisch – über algorithmische Vorhersagen über Nutzervorlieben, -verhalten usw. – abgerundet werden: Es entsteht das virtuelle Bild des realen Nutzers von Diensten im Netz – mit ganz realen Wechselwirkungen und stets steigendem Schutzbedarf.

ID-Wertkorrelation im virtuellen Raum

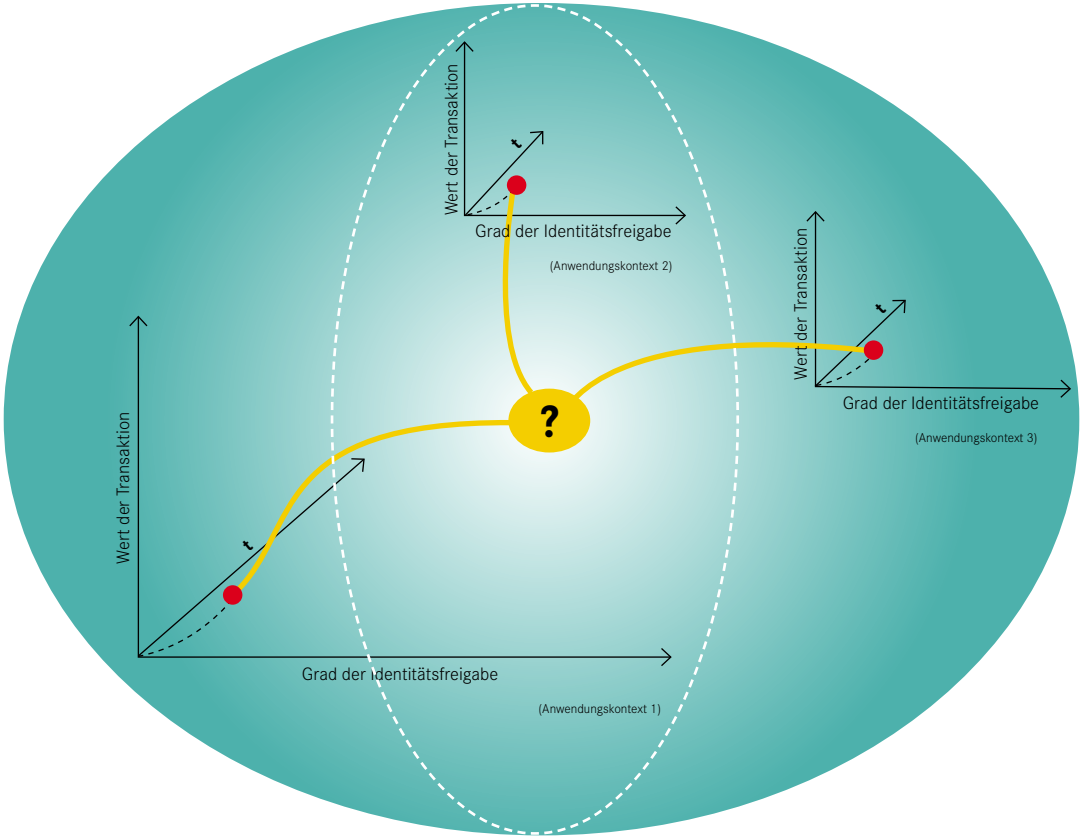


Abbildung 6: Identitätsfreigaben und Transaktionswert im virtuellen Raum

3.2 Identitäten und Sicherheit

Die oben aufgeführte Darstellung unterstreicht, dass Sicherheit (und deren entsprechende technologische Umsetzung) analog zur Werthaltigkeit einer Identität in ihrem Anwendungskontext zu definieren ist.

Sicherheit ist in diesem Modell (Abb. 5) der marktwirtschaftliche Gleichgewichtszustand, bei dem sowohl seitens des verantwortlich handelnden Nutzers als auch des Anbieters vollständige Transparenz über die Nutzungsbedingungen der gehandelten (virtuellen) Identität herrscht. Anbieter und Nachfrager verhalten sich gemäß festgeschriebener oder impliziter Normen und Konventionen, durch deren Anwendung die Integrität und Authentizität von Daten gewahrt bleiben und letztere ausschließlich den vereinbarten Einsatzzwecken vorbehalten sind. Es wird deutlich, dass somit die Faktoren Vertrauen und Verlässlichkeit der Ausgangspunkt zur Bewertung des Verhaltens der Gegenseite sind. Sie sind im Verhältnis von Anbietern und Nachfragern ebenso relevant wie in der Bewertung von (technischen) Schutzmaßnahmen gegen unberechtigte Zugriffe Dritter.

Sicherheit kann nur in einem ordnungspolitisch definierten Rahmen existieren, der den grenzüberschreitenden Charakter digitaler Dienste zu berücksichtigen hat. Die politische Verfolgung des Zielzustands »Sicherheit« wird einerseits durch Sicherheitstechnologien als technologisches, andererseits durch die individuellen Handlungen weiterer Marktteilnehmer als wertorientiertes Korrektiv begleitet.

Sicherheitsanforderungen sind in zahlreichen fachlichen Teilgebieten ausführlich beschrieben und weitgehend mit (rechtlichen) Sanktionsmechanismen hinterlegt. Wiederkehrendes Element zur kontextübergreifend erfolgreichen Verankerung von Sicherheit ist die Herstellung klarer und nachvollziehbarer **Haftungsregelungen,** basierend auf **messbaren Sicherheitskriterien**. Dabei sind kulturelle Faktoren nicht zu vernachlässigen, die sich sehr konkret bei einzelnen, in der Öffentlichkeit oft kontrovers diskutierten Teilaspekten von Internetanwendungen zeigen: Zwischen den teils rechtshistorisch, teils aus dem Verständnis des Staates begründeten datenschutzrechtlichen Sammlungen von Einzelfeldregelungen im angelsächsischen Raum bis hin zu umfassenden Datenschutzregelungen in der Europäischen Union stoßen sich zuweilen (nationale, kontinentaleuropäische) Traditionen mit dem interdependenten, grenzenlosen Charakter des Internets. Dessen strukturelle Flexibilität und Offenheit bringt gerade das Dilemma einer höheren Verwundbarkeit mit sich, so dass die Frage eines angemessenen Sicherheitsniveaus nur im jeweiligen Anwendungskontext zu definieren ist. Genau auf dem Gebiet der Sicherheitsökonometrik scheint daher derzeit umfassender Handlungsbedarf gegeben zu sein. Diesem soll bei der Themenfeldbetrachtung im Einzelnen nachgegangen werden.

Einhundertprozentige Sicherheit zu erreichen ist technisch nicht möglich. Die Übernahme einer derartigen Zielsetzung wäre ein Trugschluss: Durch die technologische Fortentwicklung kann gesamtheitlich gesehen Sicherheit nicht statisch-absolut als Ziel betrachtet werden. Ihre Erreichung muss Ziel und Anspruch bleiben und ITK-Innovationszyklen begleiten, ohne sie vorwegnehmen zu können.

Sichere Identitäten (SI) wurden im ersten Bericht der Promotorengruppe Sicherheit vom November 2010 zunächst – für die zum damaligen Zeitpunkt durchgeführte Szenarioanalyse hinreichend konkret – als themenfeldbezogene Elemente behandelt. Dabei ist zu differenzieren zwischen:

- den physischen oder virtuellen - personenbezogenen Identitäten von Personen und der fallweisen Kombinationsmöglichkeit mit weiteren personenbeziehbaren Daten und
- objektbezogenen Daten zur sicheren Identifikation (letztere werden in der nachfolgenden Betrachtung nicht schwerpunktmäßig behandelt).

Künftig dürften Mischformen durch funktionale Vernetzung (zum Beispiel die Zuordnungsmöglichkeit personenbeziehbarer Daten auf Individual- oder Gruppenebene zu Objektdaten – beispielhaft sei Smart Metering genannt) häufiger anzutreffen sein.

Deutlich stärker als bei objektbezogenen Identitäten ist in der breiten Öffentlichkeit die Sicherheit der persönlichen Identität skizziert. Relevante ITK-basierte Dienste sind in diesem Zusammenhang unter anderem:

- rechtsverbindlich online abgeschlossene Geschäfte (Bestellungen, Finanztransaktionen etc.);
- Beziehungen zwischen Bürger und Staat (elektronische Bürgerdienste);
- die eigene Darstellung in sozialen Netzwerken oder auf anderen Plattformen;
- die Übermittlung von Daten per E-Mail oder andere Datendienste;
- die Nutzung von Cloud-Diensten;
- mobile Kommunikation.

Daran schließt sich die Frage an, ob seitens des Nutzers auch eine Bereitschaft besteht, in Sicherheitslösungen zu investieren – bzw. wie der Nutzer ermutigt werden kann, entsprechende Investitionen vorzunehmen. Weiter gefasst stellt sich die Frage, ob sich neue Geschäftsmodelle im Bereich Sicherheit verorten lassen. Hierzu können lediglich Ansätze aufgezeigt werden, die in der unternehmerischen Praxis auf Tragfähigkeit als Geschäftsmodellinnovation zu prüfen sind.

3.3 Handlungsfeld Datenschutz

3.3.1 Ausgangslage

Kaum ein Themenfeld ist breiter aufgestellt, erfährt einen höheren medialen Zuspruch und wird politisch höher priorisiert als der Schutz persönlicher und personenbeziehbarer Daten in elektronischen Netzen (Privacy-Debatte). Datenschutz schafft das Vertrauen und die Akzeptanz, die für die Erhebung und Verarbeitung personenbezogener Daten in der Wissensgesellschaft unabdingbar sind. Das deutsche Datenschutzrecht beruht auf den Vorgaben zweier EU-Richtlinien: RL 95/46/EG (für das Bundesdatenschutzgesetz) und RL 2002/58/EG (für die datenschutzrechtlichen Vorschriften im Telemediengesetz und Telekommunikationsgesetz).

Verschiedene sicherheitsrelevante Vorfälle der jüngeren Vergangenheit, bei denen mangels Datensicherheit auch der Datenschutz kompromittiert wurde, zeigen zum einen die enge thematische Verflechtung innerhalb des Bereichs Sicherheit; zum anderen haben sie das Thema in der öffentlichen Wahrnehmung befördert. Politisch-regulative Eingriffe scheinen nicht mehr das allein angemessene, adäquate Instrument zu sein, um neu hinzukommende Datenschutz-Aspekte fast täglich entstehender ITK-Produkte und -Lösungen zu erfassen. Einer wie auch immer ausgeprägten »Kontrolle« des Netzes jenseits der Möglichkeiten nationaler und internationaler Strafverfolgungsbehörden (etwa im Bereich des Cybercrime) steht in weiten Teilen dessen technische Architektur entgegen.
Die aktuellen Herausforderungen gehen insofern über juristische Aspekte hinaus und berühren zum Beispiel auf dem Gebiet der Social Networks verhaltenspsychologische und soziologische Fragen wie Nutzerverhalten, den Umgang mit Identitäten usw. Mehr noch: Die generelle Frage stellt sich, wie national (oder supranational, europäisch) Positionierungen erfolgen können, die neuartige, innovative Geschäftsmodelle fördern (zum Beispiel Cloud Computing), ohne aber die Vorstellungen unseres Modells einer offenen, die Rechte des Individuums schützenden Gesellschaft preiszugeben.

Für das Thema Datenschutz ist es wichtig, Antworten auf die nachstehenden Fragestellungen zu finden:

- Definitionsbereich: Welche Produkt- und Dienstekategorien sind gemeint, wenn Datenschutz thematisiert wird?
- Welche Chancen und Risiken – aus Sicht der Sicherheit – beinhalten diese? Lassen sich darauf aufbauend gegebenenfalls neue Geschäftsmodelle entwickeln?
- Welche Maßnahmen und Handlungsempfehlungen lassen sich ableiten, um mit modernen, technik- und nutzeradäquaten Datenschutzregelungen die Wettbewerbsfähigkeit von Technologie- und Diensteanbietern in Deutschland zu sichern?

Abbildung 7: Die Top-10 der Online-Communities (Quelle: BITKOM)

3.3.2 Themen

Die Promotorengruppe ist der Ansicht, dass es sich bei den öffentlich mit Netzangeboten konnotierten Problemstellungen häufig um Ausprägungen eines entweder nicht sozialadäquaten, nicht datenschutzkonformen und damit sicherheitskompromittierenden Nutzungsverhaltens Einzelner oder um anbieterseitige Mängel handelt. Davon unbenommen sind Datenschutz- und damit Sicherheitslücken in den seltenen Fällen, die auf von vornherein nicht rechtskonformen Geschäftsmodellen beruhen.

Neu sind die technologischen Möglichkeiten – damit hauptsächlich die Geschwindigkeit der Informationsverarbeitung und die Informationsvernetzung – die dem Nutzer an die Hand gegeben werden. Ob, in welchem Umfang und wie oft er welche Dienste nutzt, bleibt ihm unbenommen. Zwischen den Extrempolen der Digital Natives, der Post-Privacy-Vertreter und denjenigen, die nicht oder nur selten Netzdienste nutzen, liegen die Eigenverantwortung des Nutzers und die anzustrebende Transparenzpflicht des rechtskonformen Diensteanbieters.

Abbildung 8: Jeder zweite Internet-Nutzer hat ein Online-Profil (Quelle: BITKOM)

Unverändert bestehen bleibt aber der Fragekanon, der losgelöst von den technischen Möglichkeiten existiert: Wie stellt sich der Einzelne nach außen dar – und definiert damit seine Identität(en)? Wie kann der Einzelne in die Lage versetzt werden, diesen Konstruktionsprozess so zu gestalten, dass er rational, reversibel und in seiner Eigenverantwortung steuerbar ist?

Generell bleibt festzuhalten: So wie im 19. Jahrhundert die Eisenbahnlinien ausgebaut wurden und zu Beginn des vergangenen Jahrhunderts die Telegraphenverbindungen, sind Informations- und Kommunikationstechnologien das technologische Rückgrat des 21. Jahrhundert. Insofern erscheint es folgerichtig, dass anknüpfend an die staatlichen und privatwirtschaftlichen Anstrengungen zum Ausbau von Breitbandinfrastrukturen und die analog wachsende Bedeutung sicherer Infrastrukturen insgesamt nunmehr Nutzer, Wirtschaft und Staat Hand in Hand arbeiten müssen, um diese Infrastrukturen zu sichern. Je nachdem, welche Anwendungen einem »informationellen Sozialstaat« und daraus folgend einem Recht auf informationelle Teilhabe zugeordnet werden und wo wiederum primär der Nutzer in der Verantwortung gesehen wird, sind die politischen Weichenstellungen vorzunehmen. Ziel muss es sein, eine generationen- und schichtenübergreifende Chancengleichheit beim Zugang zu, der Nutzung von und der Wissenserschließung durch neue Technologien zu erzielen.

Abbildung 9: Infos, Communities und Multimedia (Quelle: BITKOM)

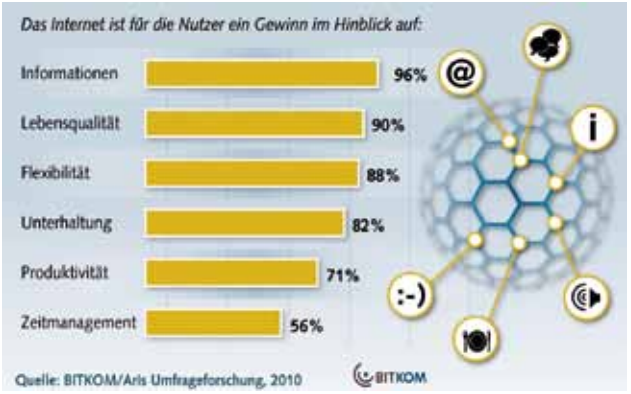


Abbildung 10: Internetnutzer begreifen das Web als Gewinn (Quelle: BITKOM)

3.3.2.1 INDIVIDUALISIERUNG VON IDENTITÄTEN

Die aktuelle Entwicklung von Identitäten zeichnet die Verschiebung der theoretischen Grundlinie einer starren, extern zugeschriebenen Identität, wie sie etwa in Geschäftskontexten verwendet wird, hin zu einer zunehmend dynamischen Definition von Identitäten aus. Gegenwärtig populäre Dienste im World Wide Web, insbesondere im Web 2.0, sind stärker relational orientiert und weniger von außen bestimmt als in der Vergangenheit.

Diese Individualisierung von Identitäten, die Selbstdarstellung im und über das Netz ist nur die Fortschreibung konventioneller Individualisierungsinstitutionen und damit mittlerweile Teil des als normentsprechend erachteten Sozialisationsprozesses. Es handelt sich dabei um keine Erscheinung, die einer bestimmten Alterskohorte zuzuschreiben wären:
Das Bedürfnis nach Privatsphäre, vielleicht graduell anders definiert, besteht bei Jugendlichen ebenso wie beim Silver Surfer.

Die Individualisierung findet ihre logischen Grenzen – und gibt damit den Anstoß zur Entwicklung neuer Geschäftsmodelle - dort,

- wo sie als zunehmende Massenerscheinung nur wenig Differenzierungsmerkmale der Dienstenutzer bieten kann, also zu einer Uniformisierung der Einzeldarstellung führt und zugleich
- der Nutzer seine »Kosten« (Datenpreisgabe, etwaige Sicherheitsrisiken) nicht mehr adäquat angebotsseitig wiedergegeben sieht (vgl. Abb. 5).

Die Reaktion deutscher Anwender bei der Nutzung von Internet-Angeboten pendelt dabei zwischen den Extrempolen »übervorsichtig« und »fahrlässig«, wie eine Studie des BITKOM nachweist. Dies zeigt deutlich den Handlungsbedarf an dieser Stelle.

Es sei an dieser Stelle hervorgehoben, dass bestimmte Erscheinungen, die gemeinhin pauschalisierend der Nutzung von Informations- und Kommunikationstechnologien zugeschrieben werden, nur oberflächlich neu sind. Die kritische Betrachtung derselben schreibt sich häufig in einen kulturpessimistischen Diskurs ein. Dieser ist weder innovativ noch hilfreich dabei, den

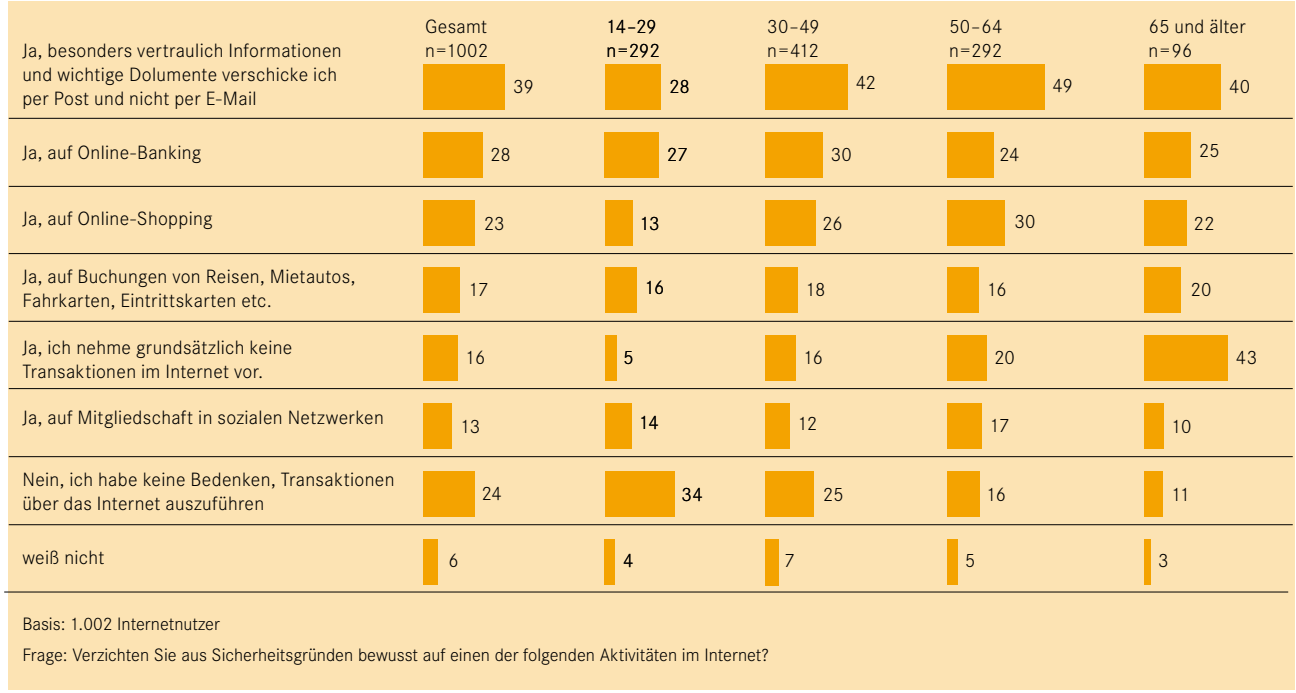


Abbildung 11: Verzicht auf Aktivitäten im Internet – nach Alter (Quelle: BITKOM)

Mehrwert und Produktivitätsgewinns durch ITK zu den in Randzonen lokalisierbaren Problembereichen in ein angemessenes Verhältnis zu setzen. Anzustreben wäre, dass über diese beobachtbare Befassung mit temporären Phänomenen hinaus beim Umgang mit individuellen Daten im Netz die folgenden Herausforderungen angegangen werden:

a. **Wie kann der Nutzer die Kontrolle über seine Daten behalten?** Wie kann die Preisgabe von Daten auch an Anbieter außerhalb des Rechtsrahmens der Europäischen Union transparent und möglicherweise auch reversibel gestaltet werden? Zu klären ist daher, wie die immer zahlreicher im Zuge der Dienstenutzung preisgegebenen und zusammengeführten persönlichen Informationen als Teil der eigenen Identität(en) vor missbräuchlicher Nutzung geschützt werden können und welche technischen Hilfsmittel dafür zur Verfügung stehen.

   In der medialen Debatte über die Erhebung und Verarbeitung von Nutzerdaten geht zuweilen auch die Differenzierung verloren, an wen Nutzerdaten weitergegeben und durch wen sie eingesehen bzw. verarbeitet werden. Aus der Perspektive der Promotorengruppe Sicherheit differenziert sich die Risikobewertung danach, ob beispielsweise lediglich der Internet Service Provider (ISP) zu Abrechnungszwecken Einsicht in bestimmte Nutzerdaten hat oder diese von einem Dienstleanbieter mit Verhaltens- und Bewegungsprofilen angereichert werden, um primär zu Werbe- oder anderen Zwecken eingesetzt zu werden.

   Aus diesen kritischen Fragestellungen ergeben sich anbieterseitig durchaus Chancen: Mit der zunehmenden Sensibilisierung von Anwendern für Fragen des Datenschutzes erhalten auch neue (Nischen-) Anbieter eine Chance, sich mit entsprechenden Lösungen zu behaupten; indirekt würden wahrscheinlich auch die am Markt etablierten Firmen dazu animiert werden, systemarchitektonisch datenschutzadäquate Modelle zu verfolgen bzw. Ansätze wie privacy by design technologisch zu untermauern.

b. Die Darstellung von Nutzern im World Wide Web – wissentlich (bspw. über die bewusste und als Mehrwert empfundene Preisgabe von Informationen in sozialen Netzwerken) und unwissentlich (über die maschinell, algorithmisch gesteuerte Zusammenführung von Nutzerdaten zu kommerziell verwendeten Nutzerprofilen, Data Mining etc.) – bringt als Sekundäreffekt auch die Veränderung sozialer Rollen- und Funktionszuschreibungen mit sich. **Wie kann eine Demokratie auf diese veränderten Kommunikations- und Repräsentationsformen reagieren?** Wie kann der bisher auf die kleine Gemeinde der Intensivnutzer des Netzes begrenzte Diskurs aufgebrochen und zu einer gesellschaftlichen Debatte, die auch ethische Grundfragen berührt, erweitert werden?

c. Wenn davon ausgegangen wird, dass die Antworten auf vorstehend geschilderte Phänomene im nationalen oder europäischen Alleingang zumindest nur teilweise lösbar sind: Wie kann das **Umfeld für neue, anforderungsadäquate Geschäftsmodelle im Web** attraktiv gestaltet werden?

3.3.2.2 NUTZERDATENINTENSIVE ANWENDUNGEN

Nutzerdatenintensive Anwendungen (von sozialen Netzwerken bis zu Geolokalisationsdiensten) sind nachweislich der Nutzerzahlen und der Umsatzdaten nachgefragte Geschäftsmodelle. In der privaten und auch beruflichen Nutzung schaffen sie vom Nutzer gewünschten Mehrwert. Dabei ist die bewusste Preisgabe persönlicher Daten ein offensichtlicher und notwendiger Teil des Angebots für den Nutzer. Sie wird aber von ihm teils indifferent bis skeptisch wahrgenommen. Ungelöst sind aber bisher die Fragen, wie die Anwendungsgrundlage (eventuell verpflichtend) für derartige Regelungen angemessen verbreitert werden kann und wie die faktische Rechtsnormdurchsetzung grenzüberschreitend gestaltet werden sollte.

Innerhalb Deutschlands und der Europäischen Union kann der Anwender in diesem Zusammenhang auf die entsprechenden Datenschutzregelungen zurückgreifen. Internationale Regelungen im Bereich des Datenschutzes existieren teilweise (zum Beispiel Safe Harbor).

Bei der oft unüberschaubaren Vielzahl von persönlichen Daten, die der durchschnittliche Nutzer bei Netzdiensten preisgibt – sowie der personenbeziehbaren Daten, die von ihm wissentlich oder unwissentlich erhoben werden – stehen ihm nur wenig Möglichkeiten zur Verfügung, den auf ihn bezogenen (unter Umständen verstreut gespeicherten, aber zusammenführbaren) Datenbestand zu kontrollieren und ggf. zu modifizieren. In Einzelfällen können jedoch die Rechte Dritter tangiert werden (zum Beispiel Benennung auf Photos in sozialen Netzwerken; etwaige Begleiteffekte beim Einchecken in bestimmten Locations).

Auch hier ist das Phänomen an sich nicht neu: Schon vor dem Informationszeitalter konnte in einem bestimmten Rahmen in Bild und Ton über Dritte berichtet werden, wurden und werden Scoring-Daten erhoben etc. Neu ist hingegen die Geschwindigkeit der Zusammenführung, ständigen Ergänzung und algorithmischen Verarbeitung von personenbezogenen und personenbeziehbaren Informationen, ohne dass diese Schritte im Einzelnen für den Nutzer nachvollziehbar oder einsehbar wären.

Es kann bei global angebotenen Diensten kraft Natur der Sache nicht darum gehen, im nationalen Alleingang regulativ tätig zu werden, wenn es sich um Begleiterscheinungen vom Nutzer gewünschter Anwendungen handelt: Vielmehr müsste und sollte dann dem veränderten Datenschutzbedürfnis des Nutzers durch frei wählbare Lösungen Rechnung getragen werden. So existieren, um ein Beispiel zu nennen, bereits heute sogenannte Cookie-Opt-Out-Lösungen als Plugin für handelsübliche Browser (zur Vermeidung bzw. Einschränkung unerwünschten Behavioral Advertising). Dem Nutzer steht es frei, diese oder ähnliche Lösungen unkompliziert zur Anpassung an sein persönliches Sicherheits- und Datenschutzbedürfnis einzusetzen.

Sofern hingegen die ungefragte, intransparente Datenanreicherung konstitutives Element international angebotener Geschäftsmodelle ist und dies als politisch diskussionswürdig erachtet wird, sollte im Rahmen internationaler Organisationen und Gremien wie G8, ICANN oder IGF überlegt werden, wie dem Erfordernis nach mehr Transparenz im Umgang mit Nutzerdaten angemessen Rechnung getragen werden kann. Ziel sollte es sein, den Nutzer auf transparente Weise auf Wunsch die Verwendungswege und -arten seiner Daten einsehen zu lassen. Der schlussendlich gewählte Ansatz darf ihn jedoch nicht paternalistisch bevormunden – informationelle Selbstbestimmung beinhaltet bewusst die Freiheit des Einzelnen, über die Verwendung seiner Daten frei zu entscheiden. Die Zusicherung von Transparenz

und Reversibilität von Nutzerdatenspeicherungen (einschließlich identitätsrelevanter Angaben) durch den Anbieter wäre ein geeigneter Ansatz, die erforderliche Balance zwischen dem staatlichen Schutzauftrag und der informationellen Selbstbestimmung herzustellen.

Sofern keine ausdrücklich entgegenlautende Willensäußerung des Nutzers existiert, sollte ferner diskutiert werden, welche **Speicherdauer** von Nutzerdaten im kommerziellen Bereich angemessen erscheint und ob nicht generell eine Obergrenze im Sinne eines »Verfalldatums« sinnvoll wäre (davon unbenommen ist die Dauer der Speicherung von Nutzerdaten zu Strafverfolgungszwecken). Die technischen Herausforderungen dürften dabei aufgrund der redundanten Internetarchitektur substantiell sein, so dass zunächst die technische Machbarkeit zu prüfen wäre.

3.3.2.3 PRIVACY-ENHANCING TECHNOLOGIES (PET)

Die **Förderung von Privacy-Enhancing-Technologies** der nächsten Generation und begleitende Schaffung der notwendigen Rechtsgrundlagen rücken zunehmend in den Fokus. Nicht zuletzt bei Nutzeraktivitäten im World Wide Web kann es hilfreich sein, Methoden der (partiellen) Anonymisierung oder Pseudonymisierung bereitzustellen, die es dem Nutzer gestatten, jeweils nur die exakt benötigte Datenmenge und -qualität zu übermitteln. Über mehrere, in ihrer technischen Dienstleistung begrenzte Trustcenter würden diese nach Nutzerbedarf gestaffelten, temporären, multiplen Identitäten bereitgestellt. Damit würde neben der rein technischen Lösung, d. h. der Einschaltung einer vertrauenswürdigen dritten Partei, voraussichtlich auch ein Sicherheitsgewinn in der Nutzerwahrnehmung zu verzeichnen sein.

FALLBEISPIEL:

Eine international tätige Unternehmensgruppe stellt für die Werbewirtschaft geeignete Nutzungsprofile im World Wide Web zusammen. Um dabei datenschutzkonform im jeweils relevanten Rechtsraum zu handeln und keine Verbindung dieser Daten zu tatsächlichen Personen oder auch nur bestimmten IP-Adressen herzustellen, wird eine durch eine dritte Partei betriebene Black-Box eingesetzt. Diese Dienstleistung gewährleistet die Entkopplung von potentiellen Nutzer- und Nutzungsdaten. Dadurch wird datenschutzkonform die Entwicklung neuer Geschäftsmodelle gewährleistet.

Für Deutschland als potentiellen Standort derartiger Drittanbieter werden aufgrund seiner internationalen Reputation als vertrauenswürdiger Akteur im Bereich Sicherheit als auch wegen der hier verorteten technologischen Kompetenz gute Chancen gesehen.

Offen sind derzeit aber noch rechtliche Fragen, die in der »analogen« Welt beschrieben sind: Wie kann beispielsweise bei Problemen der Vertragserfüllung zweier kontrahierender Parteien, von denen eine aus Sicherheitsgründen bewusst nur eine Teilidentität bei Vertragsschluss eingesetzt hat, die reale Person identifiziert werden? Sollten dafür automatische Durchgriffsmechanismen auf die vollständige Identität vorgesehen werden? Wie können bereits vor Vertragsschluss auf transparente Art und Weise die Bedingungen definiert werden, unter denen Teilidentitäten aufgelöst werden?

Augenmerk sollte auch auf die Frage gerichtet werden, wie – aus institutionenökonomischer Sicht – zeitnah Netzwerkeffekte erzielt werden können. Das heißt: Wie können potentiell für den Einsatz von Teilidentitäten geeignete Diensteanbieter dazu bewogen werden, ohne einen Nachfrager-Kundenstamm ihre Dienste entsprechend zu konfigurieren? Oder aus Nutzersicht: Wie kann der Nutzer zum Einsatz neuartiger ITK-Technologien gebracht werden, ohne dass das Komplementärgut für eine ITK-basierte Identität vorhanden ist? Der Schlüssel dafür scheint in der externen Anreizsetzung durch systemisch sicherheitsinteressierte Dritte zu liegen, insbesondere durch den Staat, um dem in der Startphase schwer marktfähigen, abstrakten Gut Sicherheit über die Wahrnehmungsschwelle hinwegzuhelfen und im Sinne positiver Netzwerkeffekte einer breiten Nutzung zuzuführen. Zu erörtern wäre beispielsweise, ob Elemente des Entwurfs der »National Strategy for Trusted Identities in Cyberspace« (USA 2010) auch im deutschen Kontext als sinnvolle Anreizsetzung in Frage kämen. Genannt werden »Steuervergünstigungen, Cybersecurity-Versicherungen, Förderprogamme oder Darlehen für Erstanwender.«

Vertrauensbildende Maßnahmen seitens der Diensteanbieter könnten beispielsweise ein freiwilliges Privacy-Impact-Assessment vorsehen. Diese Qualitätssicherungsmethode würde transparent aufzeigen, welche etwaigen Datenschutzrisiken ein System oder dessen datenschutzrelevante Komponenten beinhalten. Durch regelmäßige Überprüfungen würde dem technischen Fortschritt entsprochen. Der Nutzer bekäme damit einen Indikator beigestellt, der ihm die freie und verantwortungsvolle Wahl von Diensten und Anbietern erleichtert.

EXKURS: GASTBEITRAG PROF. DR. JOHANNES BUCHMANN

PRIVATSPHÄRE IM INTERNET – HERAUSFORDERUNGEN UND SCHUTZMÖGLICHKEITEN

Herausforderungen

Die Informations- und Kommunikationstechnologie durchdringt alle Lebensbereiche. Große öffentliche Datenbanken entstehen seit langem in vielen Bereichen, zum Beispiel in der Gesundheitsversorgung, im Steuerwesen und in der Gerichtsbarkeit. Sensoren, RFIDs, mobile Endgeräte und Überwachungskameras bilden die physische Welt in der digitalen ab und machen Monitoring und Tracking von Personen möglich. Dies wird zum Beispiel zur Erhöhung der Sicherheit in öffentlichen Räumen wie Bahnhöfen und Flughäfen und zunehmend auch bei der Betreuung alter und kranker Menschen eingesetzt. Daten werden in sozialen Netzwerken wie Facebook, Flickr, YouTube und MySpace von Endbenutzern für Endbenutzer generiert, beliebig und auf Dauer gespeichert, ausgetauscht und weiterverwendet. All diese Daten und Informationen können durch mächtige Suche- und Analysewerkzeuge erschlossen werden. Unternehmen wie eFindOutTheTruth.com und LexisNexis bieten Produkte und Dienstleistungen an, die darauf beruhen.

Traditionelle Vorstellungen von Privatsphäre und Strategien, die Menschen traditionell zum Schutz ihrer Privatsphäre angewendet haben, lassen sich kaum in diese digitale Welt übertragen. Menschen handeln in verschiedenen Kontexten und sind bisher davon ausgegangen, dass ihr Handeln in einem Kontext keine Auswirkung auf ihr Handeln in anderen Kontexten hat. Wie Helen Nissenbaum in ihrem Buch »Privacy in Context« dargestellt hat, ist dies in der digitalen Welt völlig anders. Kontexte lassen sich kaum definieren und voneinander trennen (Nissenbaum, 2009). So glauben Menschen traditionell, sie seien anonym, solange sie sich in bestimmten Kontexten nicht identifizieren. Im Internet hinterlassen sie aber eine breite und lebenslang zugreifbare Datenspur, anhand derer sie oft auch nachträglich noch identifizierbar sind. (Rao & Rohatgi, 2000).

Entsprechend verunsichert sind viele Menschen. In einer Befragung von 5.030 deutschsprachigen Bürgern (Dörflinger, 2009) geben 60% der Befragten an, dass sie Überwachung bzw. Ausspähung der eigenen Privatsphäre im Internet befürchten und kaum Möglichkeiten sehen, die eigenen Daten kontrollieren zu können.

Schutzmöglichkeiten

Schutz der Privatsphäre im Internet setzt voraus, dass die individuellen und gesellschaftlichen Anforderungen an diesen Schutz differenziert nach Kontexten bekannt sind und ein gesellschaftliches Bewusstsein für diese Differenzierung entsteht. Dies ist auch und gerade für die wirtschaftliche Entwicklung wichtig, weil der Wegfall von abgegrenzten Vertrauensbereichen (De-Perimetrisierung) langfristig zur Herausbildung monopolartiger Machtverhältnisse mit wirtschaftlichen Nachteilen führen kann. Erst die Differenzierung macht eine Umsetzung möglich, die nicht die wirtschaftliche Entwicklung behindert, weil sie nur dort Ressourcen investiert, wo dies geboten ist. Eine Herausbildung von globalen, mindestens aber europäischen rechtlichen Standards, ist entscheidend. Technik kann dann ein verantwortungsvolles und transparentes Datenschutzmanagement zum Beispiel durch Datenminimierung und ein benutzbares Identitätsmanagement unterstützen. Gerade im Bereich des Identitätsmanagements ist die Deutsche Forschung und Entwicklung international führend. Technisch hervorragende Lösungen existieren. Ein wichtiger Fokus wird in der Zukunft auf der einfachen Benutzbarkeit liegen müssen.

3.3.2.4 DATENSCHUTZRECHT

Datenschutzbestimmungen definieren die Regeln zum Umgang mit persönlichen und zunehmend auch personenbeziehbaren Daten. Sie unterstützen das individuelle Recht auf informationelle Selbstbestimmung auch dort, wo nach allgemeinem Dafürhalten ein durchgehendes Selbstschutzbewusstsein und -interesse der Bürger vermutet werden können.

Datenschutzbestimmungen sind normativ gesetzt. Ein absolutes Schutzniveau existiert nicht; das Datenschutzbedürfnis (in einer teilweisen Schnittmenge mit dem funktionalen Bedürfnis nach IT-Sicherheit) einzelner Nutzer, Nutzergruppen, Bürger oder des Staates kann dabei nicht zwangsläufig deckungsgleich sein. Ganz im Gegenteil können die entsprechenden Interessen diametral zueinander stehen. Dabei entsteht ein zusätzliches Spannungsverhältnis zwischen Sicherheitsbedarf, (technologischen) Möglichkeiten zur Gewährleistung von Sicherheit und dem heute statischen, wenig flexiblen Datenschutzrecht. Dieses differenziert in Deutschland derzeit wenig zwischen qualitativ unterschiedlichen Schutzsphären und damit verschiedenen Schutzbedürfnissen und einer analog qualitativen Datenschutzabstufung mit einem im Zweifelsfalle höheren Schutzniveau für den Nutzer.

Aus einigen der vorhergehend aufgeführten Beispiele kristallisiert sich heraus, dass die aktuell gültige Datenschutz-Gesetzgebung mit der raschen technologischen Entwicklung im Bereich der Informations- und Kommunikationstechnologien seit den achtziger und neunziger Jahren des vergangenen Jahrhunderts in Teilbereichen nicht Schritt halten konnte. Dem zugrunde liegt ein technologischer Paradigmenwechsel, der in dieser Form vor einigen Jahrzehnten nicht vorhersehbar war.

GRUNDPRINZIPIEN DES DATENSCHUTZES IN DER »ERKLÄRUNG VON MONTREUX«:

- Prinzip der Zulässigkeit und Rechtmäßigkeit der Erhebung und Verarbeitung der Daten,
- Prinzip der Richtigkeit,
- Prinzip der Zweckgebundenheit,
- Prinzip der Verhältnismäßigkeit,
- Prinzip der Transparenz,
- Prinzip der individuellen Mitsprache und namentlich der Garantie des Zugriffsrechts für die betroffenen Personen,
- Prinzip der Nicht-Diskriminierung,
- Prinzip der Sicherheit,
- Prinzip der Haftung,
- Prinzip einer unabhängigen Überwachung und gesetzlicher Sanktionen,
- Prinzip des angemessenen Schutzniveaus bei grenzüberschreitendem Datenverkehr.

Quelle: http://www.lda.brandenburg.de/sixcms/detail php?gsid=lbm1.c. 297384.de &template=lda_entschl

Sicherheits- und (als teilweise Schnittmenge) Datenschutzanforderungen konnten noch in den achtziger Jahren einfacher und stringenter in langzyklisch angelegte Software-Entwicklungsprozesse eingebunden werden. Typischerweise wurde die Systemarchitektur vom Programmierer ex ante entworfen; Datenschutzanforderungen setzten bereits bei der Definition der Entwicklungsziele und der darauf aufbauenden (technischen) Spezifikationen an. Diese Vorgehensweise ist in der Regel formalisiert

und funktioniert dann hervorragend, wenn Änderungsanforderungen noch im Prozessdesign berücksichtigt werden können und insgesamt die Innovationszyklen eher lang angelegt sind.

Mit steigender Rechenleistung und einer veränderten Nachfrage der Anwender ändert sich dieser Ansatz ab den neunziger Jahren (»Release often, release early.«) Früher starre systemarchitektonische Grenzen werden heute zunehmend aufgeweicht (zum Beispiel SOA, Cloud Computing, SaaS), um beispielsweise unternehmensübergreifend Prozesse modellieren zu können.

Im privaten Bereich – mit der Kreativität von Abermillionen Programmierern – bieten ITK die Möglichkeit, auch mit begrenzten Programmierfähigkeiten aus der Verknüpfung existierender Softwarebibliotheken in kürzester Zeit und endgeräteübergreifend (PC, Smartphone, Tablet-PC) neue Dienste zu kreieren. Dieses Phänomen kennzeichnet auch einen fundamentalen kulturellen Wandel: Der Nutzer wird vom Konsumenten digitaler Angebote nunmehr auch zum Produzenten. Datenschutzanforderungen, die in diesen neuen Ansätzen auf Komponenten- bzw. Subsystemebene berücksichtigt werden können, sind systembedingt nicht notwendigerweise durch die bedarfsgerecht abrufbaren oder modular entstandenen Programme erfüllt.

Die Promotorengruppe Sicherheit empfiehlt, diese Diskussionen unter Einbeziehung aller relevanten Stakeholder zu forcieren. Zielsetzung wäre dabei, dem oben aufgeführten technologischen Paradigmenwechsel dergestalt zu entsprechen, dass im Datenschutzrecht die bisherige Logik der quantitativen Begrenzung des Datenaustausches durch eine der heutigen Wirklichkeit eher entsprechende qualitative Schutzniveauabstufung ersetzt würde.

Das bedeutet konkret, vom Verständnis des Datenschutzes hin zu einem Verständnis des Informationsschutzes zu gelangen: Nur die wenigsten Angriffe auf IT-Systeme sind auf Daten per se orientiert. Vielmehr liegt dort wie auch bei der Zusammenführung von Einzeldaten als Geschäftsmodell der Fokus darauf, welche Informationen sich aus den gewonnenen Daten generieren und dann als Wissen zusammenführen lassen. Ein entsprechend aufgebautes Informationsschutzrecht würde an sich sensible Daten wie bisher auch mit hohen Schutzanforderungen versehen. Ein Datum hingegen, das weder für sich genommen noch im Verhältnis zu anderen Daten eine Missbrauchswahrscheinlichkeit aufweist und nicht einzelnen Personen zugeordnet werden kann, würde entsprechend seines Schutzbedarfs abgestuft behandelt.

Zur Adressierung der Thematik in international aufgestellten Unternehmen kann nach Auffassung der Promotorengruppe Sicherheit das deutsche Rechtsmodell durchaus Chancen für positive Alleinstellungsmerkmale im Wettbewerb bieten. Unternehmen, die europäische und deutsche Datenschutzanforderungen erfüllen, dürften beim interessierten Anwender einen erheblichen Vertrauensvorschuss genießen. Wettbewerblich wären sie weltweit dann im Vorteil, da sie bereits europäische und deutsche Schutzanforderungen erfüllen. Um der Vielfalt der Anwendungsfälle in den jeweiligen Marktsegmenten gerecht zu werden, sollte die Schutzintensität über die gesetzlichen Vorgaben hinaus den jeweiligen Anbietern pragmatisch überlassen werden.

3.3.3 Handlungsempfehlungen

- **Nutzersensibilisierung und Herstellung von Transparenz.** Nutzer von Netzangeboten, deren Kernfunktionalität auf der Freigabe persönlicher Daten beruht, sollten über ihre Rechte, Pflichten und mögliche Nutzungsrisiken in allgemeinverständlicher, nichttechnischer Sprache hingewiesen werden. Dazu gehören nicht zuletzt die nachhaltige Sensibilisierung des privaten Nutzers zu Chancen und Risiken seiner Aktivitäten sowie die Hinführung zur Datensparsamkeit.
  Die Nutzer haben dadurch weiterhin das notwendige Vertrauen, Netze – insbesondere das World Wide Web – als Zugangsmedium zur Wissensgesellschaft sicher zu nutzen.

- **Eigenverantwortung der Nutzer stärken.** Um dem Nutzer die Wahrnehmung seiner Rechte zu erleichtern, benötigt er Transparenz darüber, was mit seinen Daten geschieht. Anbieter, die diese Transparenz über das rechtsverbindliche Maß hinaus darstellen, könnten daraus Wettbewerbsvorteile durch die Schaffung von Vertrauen beim Nutzer generieren.

- **Usability durch Technologie verbessern.** Ergänzend sollten dem Nutzer von ihm handhabbare und akzeptierte (usability) technische Hilfsmittel zur Hand gegeben werden. Dazu gehört nicht zuletzt, den bereits heute mit einer Vielzahl von Passwörtern und Identifizierungsmechanismen vielfach belasteten Nutzer nicht weiter zu überfordern. Sicherheit ist kein Selbstzweck, sondern soll den Nutzer befähigen, seine Entscheidungsautonomie wahrzunehmen. Ein Beispiel: Der durchschnittliche Nutzer wird bei der Frage, ob er Sicherheitszertifikate einer bestimmten Webseite akzeptiert, in der Mehrzahl der Fälle weder das technische Wissen besitzen noch über die Zeit und Bereitschaft verfügen, Zertifikate oder Signaturen zu prüfen. Aus dem ursprünglich beabsichtigten Sicherheitsmechanismus erwachsen damit ein geringerer Nutzerkomfort, eine verminderte Nutzerakzeptanz und damit möglicherweise auch eine systemische Sicherheitslücke. Die genannten Hilfsmittel sollen ihm insofern unkompliziert und sicher die Wahrung seiner Privatsphäre in verschiedenen Anwendungskontexten gestatten. Sie sind und bleiben aber Hilfsmittel, die ein grundsätzliches Vertrauensverhältnis zwischen Nutzer und Diensteanbieter ergänzen, nicht aber ersetzen können.

- **Änderung von Identitäten im Netz erleichtern.** Dem Nutzer sind Möglichkeiten zur Hand zu geben, seine in Netzen preisgegebene(n) Identität(en) jederzeit ändern oder löschen zu können. Dies schließt die Möglichkeit zur pseudonymisierten und anonymisierten Darstellung in Angeboten des World Wide Web ein.

- **Deutsche Anforderungen als Wettbewerbsvorteil nutzen.** Die im Vergleich zu anderen Rechtssystemen strikteren Datenschutzanforderungen des deutschen Rechtsraums sollten stärker als bisher von deutschen Anbietern entsprechender Lösungen als Alleinstellungsmerkmal im Export herausgestellt werden.

- **Deutsche Innovationsführerschaft in Leitmärkten weltweit ausbauen.** Technologisch im weltweiten Vergleich führende Lösungen deutscher Anbieter zur sicheren Identifikation sollten mit Unterstützung des öffentlichen Sektors international vermarktet werden. Zur schnelleren Aufnahme durch den Nutzer und Diensteanbieter aus der Wirtschaft kann die Anreizsetzung durch den Staat hilfreich sein.

- **Datenschutzrecht anpassen und informationelle Selbstbestimmung stärken.** Das gegenwärtige Datenschutzrecht sollte zu einem umfassenderen Recht auf Informationsschutz ausgeweitet werden. Dafür sind entsprechende Produkt- und Dienstekategorien zu definieren. Mit dieser Maßnahme würde der fortschreitenden technologischen Entwicklung Rechnung getragen werden.
  Durch dynamische Präzisierung der rechtlichen Vorgaben für die Informationsaufnahme, -übermittlung und –verarbeitung wird die individuelle Freiheit gestärkt. Die durch den Nutzer wahrgenommene Sicherheit beim Umgang mit Identitäten wird gestärkt. Die entsprechenden Abstimmungsprozesse sind zur besseren Durchsetzbarkeit international abzustimmen und zu implementieren.

- **Wissensgesellschaft und Demokratie stärker verbinden.** Aus dem parlamentarischen Umfeld heraus initiierte Foren wie die Enquête-Kommission »Internet und digitale Gesellschaft« belegen die gesellschaftliche Relevanz netz- und identitätsbasierter Themen. Sie werfen gleichzeitig die Frage auf, wie das große Potential junger, technologieaffiner und innovativer Bürger stärker als bisher für partizipative Demokratie und bürgerschaftliches Engagement gewonnen werden können. Dazu sollte untersucht werden, welche elektronisch gestützten Beteiligungsformen (eDemocracy) rechtskonform und auf freiwilliger Basis sinnvoll genutzt werden können. Bewährte Praktiken anderer Staaten sind in die Analyse einzubeziehen.

Zur Erreichnung des Zielzustandes:
- Nutzersensibilisierung
- F&E zur Bereitstellung sicherheitsfördernder technischer Hilfsmittel
- Nutzerfokussierung bei Lösungsdesign
- Netzwerkeffekte / Sicherheitszugewinn durch Erschließung neuer Marktsegmente

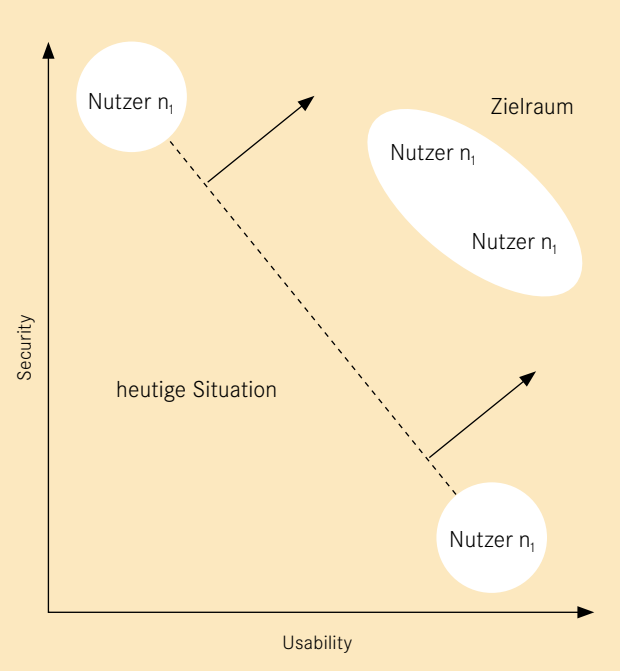


Abbildung 12: Security-Usability-Kompromiss (Annahme: Safety konstant)

3.4 Handlungsfeld Datensicherheit

3.4.1 Ausgangslage

Deutschland hält – als einige von wenigen Nationen weltweit – die industrielle Fähigkeit zur Verschlüsselung von Daten vor. Mit der steigenden Werthaltigkeit der über das Netz übertragenen (oder in der Cloud ausgelagerten) Daten, die Relevanz für Personen, Objekte oder beispielweise Fertigungsprozesse haben, steigt der Anreiz, Angriffe über Netze zu unternehmen bzw. Netze zu stören. Dies könnte sowohl über konventionelle (Netzabschaltung, DoS, Botnetze, Trojaner usw.) Verfahren als auch beispielsweise über Manipulation ungesicherter Zugriffsmöglichkeiten bei Maschinen und Anlagen (Fernwartung) geschehen.

Die Angriffs- und Störmöglichkeiten differenzieren sich fortwährend aus und folgen der technologischen Entwicklung: Vom Phishing über Skimming bis hin zur Ausnutzung von Browserschwachstellen vor dem Hintergrund der zunehmenden Nutzung ausgelagerter Programme selbst im Bereich der Standard-Bürosoftware. Mit der Adressraumerweiterung via IPv6 werden sich neue Angriffsszenarien ergeben, zum Beispiel durch Tunneling von Informationen. Dadurch wird auch die Sicherheitsbewertung, zum Beispiel mit Blick auf die Prüfung von Datenauthentizität und Authorisierung der Durchleitung, wahrnehmbar schwieriger.

Die Frage ist daher, wie die negativen Externalitäten der technologisch per se neutralen weltweiten Vernetzung eingedämmt werden können. Dies beinhaltet die Frage, welche Mechanismen sich zur nachhaltigen Vermeidung derartiger sozialer Fehlallokationen anbieten und welche sozialen oder wirtschaftlichen Anreize entsprechend gesetzt werden sollten.

FALLBEISPIEL:

Im Dezember 2008 wurde ein Seekabel, welches einen erheblichen Teil des Datenverkehrs in der Region transportierte, vor der ägyptischen Küste beschädigt. Der mehrtägige Ausfall der Übertragungskapazität war bis nach Indien spürbar, dessen Outsourcing-Industrie mit einer laut Medienberichten um 50-60% niedrigeren Übertragungskapazität zu kämpfen hatte.

Die staatliche Abschaltung von internationalen Mobilfunkdiensten in Ägypten im Februar 2011 erstreckte sich über fünf Tage. Nach Einschätzungen der OECD hatte dies direkte negative wirtschaftliche Auswirkungen von ca. 90 Millionen US-$ zur Folge.

Die Promotorengruppe Sicherheit empfiehlt mit Hilfe eines Aktionsplans zu untersuchen, wie mit Hilfe deutscher IT-Sicherheitskompetenz auch in Zukunft ein hohes Schutzniveau gegenüber unerlaubtem Zugang zu (sensiblen) Daten gewährleistet und damit deren Integrität gesichert werden kann.

EXKURS: GASTBEITRAG DR. HEIKO ROSSNAGEL

WIRTSCHAFTLICHKEIT VON SICHERHEIT – ENTWICKLUNG TRAGFÄHIGER SICHERHEITSLÖSUNGEN

Herausforderungen

Firmen oder Forschungsprojekte entwickeln technische Lösungen, die Fragen in den Bereichen Sicherheit, Privatsphärenschutz und Zuverlässigkeit adressieren. Häufig fehlt diesen Technologien aber ein Bezug zu realen Marktbedürfnissen, Nutzerwünschen und dem wirtschaftlichen Kontext. Die Folge ist, dass viele Sicherheitstechnologien in den letzen Jahren am Markt erfolglos waren. Wirtschaftliche Belange werden häufig von den Entwicklern missachtet. Stattdessen werden Sicherheitslösungen weiterhin mit einem rein technischen Fokus entwickelt, bei dem mehr Wert auf Sicherheitsgarantien und manchmal sogar Komplexität gelegt wird als auf praktische Relevanz. Die zugrundeliegende Annahme ist, dass sich diese Technologien aufgrund ihrer technischen Ausgereiftheit und der Eleganz ihres Designs automatisch am Markt durchsetzen werden. Die daraus resultierenden Geschäftsmodelle sind üblicherweise mangelhaft und nicht in der Lage, wichtige Erfolgsfaktoren entsprechend zu berücksichtigen. Kosten und Nutzen der Sicherheitslösung sind oft ungleich verteilt, was dazu führen kann, dass für die Nutzer kein Anreiz zum Einsatz der Technologie besteht. Oft berücksichtigen die Anbieter auch nicht die Zahlungsbereitschaft der Nutzer bei der Entwicklung ihrer Preismodelle, was letztendlich zum ausbleibenden Markterfolg führt. Darüber hinaus werden häufig Nutzeranforderungen wie einfache Bedienbarkeit und Zugänglichkeit ignoriert oder auch die falschen Zielgruppen angesprochen. Tragfähige Sicherheitslösungen müssen die Anforderungen aller beteiligten Parteien berücksichtigen, um sich durchzusetzen und es ist die Aufgabe der Systementwickler sicherzustellen, dass ihr System auch zu einem reellen Sicherheitsgewinn in der Praxis beiträgt.

Tragfähige Sicherheitslösungen

Um zu tragfähigen Sicherheitslösungen zu kommen, müssen die Entwickler sicherstellen, dass ihre Lösung eine effektive Sicherheitsverbesserung darstellt und sich an den Bedürfnissen des Marktes orientiert. Wenn eine dieser Anforderungen nicht erfüllt werden kann, wird es in der Praxis auch zu keiner Sicherheitsverbesserung führen. Im Bereich der Wirtschaftswissenschaften gibt es ein breites Spektrum an Methoden und Theorien, das von qualitativen Ansätzen wie der Stakeholder-Analyse oder der Diffusions- und Adoptionstheorie bis hin zu quantitativen Methoden zur Messung von Zahlungsbereitschaften reicht. Allerdings sind diese Methoden bisher kaum auf Sicherheitslösungen angewendet worden. Den Entwicklern in diesem Bereich steht also bisher kein ausgereifter Methoden-Werkzeugkasten zur Verfügung. Damit ist es für die Entwickler möglich wird, bereits in frühen Phasen des Entwicklungsprozesses die wirtschaftlichen Anforderung zu erheben und im weiteren Verlauf der Entwicklung zu berücksichtigen, ist hier noch erheblicher Forschungsbedarf vorhanden. Die Potentiale sind sehr groß: Nicht nur ist mit der Entwicklung wesentlich marktkompatiblerer Sicherheitslösungen zu rechnen, darüber hinaus können weniger erfolgversprechende Lösungen zukünftig potentiell schon in frühen Phasen der Entwicklung erkannt und aussortiert werden.

3.4.2 Themen

1. Das Thema **Verschlüsselung** liegt **im Kernbereich der staatlichen Souveränität und des hoheitlichen Interesses**. Daher scheint die Unterstützung der Forschungsanstrengungen der Unternehmen (und kooperierender Hochschuleinrichtungen sowie außeruniversitärer Forschungseinrichtungen) nicht nur sinnvoll, sondern zwingend. Dadurch werden Kompetenzen in einem spezifischen Marktsegment erhalten und ausgebaut, das einen Kern der Sicherung der staatlichen Souveränität darstellt, im Business-Bereich in den erfolgreichen Wirkbetrieb überführt werden kann und unter Beachtung der geltenden Ausfuhrbestimmungen auch für den Ausbau der Exportfähigkeit der deutschen Wirtschaft relevant ist.

   Angesichts massiver Investitionen befreundeter oder auch im Systemvergleich konkurrierender Nationen in defensive und vermutlich offensive Methoden des Datenzugriffs besteht **dringender Handlungsbedarf** in Deutschland. Dabei sollte zum einen die anwendungsorientierte, kurzfristig durch Staat und Industrie nutzbare Kompetenz auf dem Gebiet der Kryptosystemtechnologie gefördert werden (Task-Technology-Fit). Knappe Ressourcen sind dabei zu bündeln, um Effizienzverluste durch eine zu große Akteursvielfalt in diesem Nischenmarkt zu begrenzen. Die notwendige Rolle des Staates wird dabei nicht nur als Nachfrager – und in diesem Zusammenhang als Nutzer innovativer Technologien – gesehen. Seine Rolle ist dabei auch die eines Befähigers, der Technologieanbietern bzw. Forschern in marktbedingt kleineren Segmenten dabei hilft, ihre Technologien der internationalen Vermarktungsfähigkeit zuzuführen. Das zur Verfügung stehende außenwirtschaftliche Instrumentarium sollte ressortübergreifend konzentriert und auf Zielmärkte fokussiert proaktiv umgesetzt werden.

   Forschungsbedarf wird kurz- und mittelfristig nicht zuletzt in der Definition minimal-invasiver, performanter und technologisch barrierefreier Kryptomechanismen im industriellen Anwendungskontext gesehen, um bei national als sicherheitsrelevant erachteten Industriezweigen einen störungsfreien, sicheren Betrieb, gestützt auf vertrauenswürdige Daten, zu gewährleisten.

   Langfristig sind technologische Foresight-Prozesse zu stärken, damit Themen wie beispielsweise Quantenkryptographie, Post-Quantum-Cryptography, homomorphe Verschlüsselung etc. – alle heute noch nicht industriell nachhaltig nutzbar – aufgegriffen und industriell verwertet werden können.

   Sämtlicher im Rahmen eines Aktionsplans zu erarbeitender Forschungsbedarf wird nicht nur die Kompetenz der unmittelbar damit befassten Akteure stärken, sondern sichert zusätzlich Wertschöpfung in und aus deutschen Industriezweigen durch die Bereitstellung geeigneter technologischer Schutzmaßnahmen. Der Aktionsplan sollte durch die Promotorengruppe Sicherheit in Zusammenarbeit mit BMI und BMBF entwickelt werden.

2. Informations- und Kommunikationstechnologien tragen wesentlich zu dem physischen und virtuellen Schutz von kritischen Infrastrukturen und Anlagen bei. Dazu zählen unter anderem Prozesse wie die sichere Personenidentifikation und der Zugang zu Anlagen, die Verwaltung von Zugriffs- und Eingriffsberechtigungen im Rahmen eines umfassenden Sicher-

EXKURS: GASTBEITRAG PROF. JÖRG SCHWENK

BROWSER ALS SICHERE CLIENTSOFTWARE?

Moderne Webbrowser werden heute in vielen sicherheitskritischen Anwendungen als Clientkomponente eingesetzt, vom Webshop bis hin zur eID-Funktion des neuen Personalausweises. Diese Rolle kann man »historisch« (die Entwicklung der Browser seit 2004) am Beispiel Online-Banking analysieren, und zukünftige Entwicklungen am Beispiel Cloud Computing prognostizieren.

Nach Aussagen von Banken war Online-Banking bis 2004 schadensfrei; danach setzte eine massive Angriffswelle (Phishing, Pharming, Malware) ein, die browserbasiertes Onlinebanking zum Ziel hatte. Das Problem war seit langem (Felten 1997) bekannt: Layout und Funktionalität von regulären Webseiten kann von einem Angreifer mit minimalem Aufwand auf den eigenen Server übertragen werden, potenzielle Opfer können keine Unterschiede erkennen. Der vielgepriesene Schutzmechanismus SSL versagte hier völlig, da die Visualisierung der Sicherheitseigenschaften in allen Browsern ungenügend war (ein »https« statt »http«, und ein winziges Vorhängeschlosssymbol), und bei einigen Browsern (IE6) ebenfalls gefälscht werden konnte.

Im Bereich der Visualisierung von SSL sind mittlerweile große Fortschritte erzielt worden: Anzeigeelemente wurde verschoben und vergrößert, neue Typen von SSL-Serverzertifikaten (EV-Zertifikate) und ein System von Ampelfarben eingeführt (rot-gelb/weiss-grün). Dies reichte jedoch nicht aus, um das klassische Onlinebanking zu retten: Die Postbank, nach eigenen Angaben der größte Anbieter von Onlinebanking, schaffte 2011 das iTAN-Verfahren ab, und setzt jetzt auf die Sicherheit von Handys (mobileTAN) oder Chipkarten (chipTAN).

Die Gründe für diese Entscheidung sind für Fachleute leicht nachzuvollziehen: Der Browser ist zusammen mit seinen diversen Plugins (insbesondere Adobe) zu einem Haupteinfallstor für Angriffe geworden. Fast täglich werden neue XSS- und CSRF-Angriffe entdeckt, und bei bis zu 80.000 neuen Malwaresamples pro Tag darf darüber spekuliert werden, ob in Zukunft nicht für jeden einzelnen Besucher einer Webseite (Drive-by-Download) eine eigene Variante erzeugt wird. Es gibt auch keinerlei Bestrebungen, einen »sicheren« Browser zu entwickeln; vielmehr wurde die Entwicklung von XHTML zugunsten von HTML5 aufgegeben, was eine Fülle neuer Angriffsvektoren mit sich bringt.

Trotz dieser Entwicklungen ist die Popularität von Webbrowsern als Sicherheitswerkzeug ungebrochen: Web 2.0-Dienste wie Facebook, die personenbezogene Daten verarbeiten, Auktions- oder Spieleplattformen, über die geldwerte (virtuelle) Gegenstände gehandelt werden, und nicht zuletzt Cloud-Computing-Anbieter nutzen den Browser als universell einsetzbare Clientsoftware. Besonders im Bereich des Cloud-Computing ist diese Entwicklung als äußerst kritisch zu bewerten: Browser und ihre Host-Systeme sind hier den gleichen Angriffen wie im Onlinebanking ausgesetzt, und nach einem erfolgreichen Angriff besitzt der Täter vollständigen Zugriff auf alle in der Cloud gespeicherten Daten des Unternehmens. Hier ist es nicht schwer, sich kommerziell motivierte Angriffe vorzustellen: Das Spektrum reicht von simplen Erpressungsversuchen (»Zahlen Sie, oder wir löschen Ihre Daten in der Cloud«) bis hin zu gezielter Industriespionage.

Es ist unrealistisch anzunehmen, man könnte hier im nationalen Alleingang einen »sicheren Browser« entwickeln. Ziel muss es vielmehr sein, die Sicherheitsprobleme des Browsers besser zu verstehen, und in Kooperation mit internationalen Organisationen (Mozilla Foundation, OWASP, ...) nach Lösungen zu suchen.

heitskonzepts, der sichere Betrieb einschließlich sicherer Mess-, Steuer- und Regeltechnik.

Der überwiegende Teil kritischer Infrastrukturen (Netze) befindet sich in Deutschland in privaten Händen. Die Funktionsfähigkeit dieser Infrastrukturen ist für Deutschlands Sicherheit vor dem Hintergrund der latenten Bedrohungslage vital. Von der Presse den Bereichen Cybercrime bzw. Cyberwar zuschriebene Angriffe wie »Stuxnet« zeigen jedoch, dass auch bislang sicher eingeschätzte, weniger untersuchte Elemente kritischer Infrastrukturen, nicht zuletzt die Stromversorgung, neu bewertet werden müssen. Politisch wurde darauf u. a. bereits mit der Schaffung des Nationalen Cyber-Abwehrzentrums (NCAZ) reagiert.

3.4.3 Handlungsempfehlungen

1. Der Ausdifferenzierung der Angriffsszenarien (IT-Kriminalität sowie staatlich gelenkte Angriffe) und –möglichkeiten muss bei der Auswahl der Gegenmaßnahmen Rechnung getragen werden. Dazu gehört in diesem Kernbereich staatlicher Sicherheit nicht zuletzt, **nationale Kernfähigkeiten** der IT-Sicherheit zu definieren. In einem zweiten Schritt ist daraus abzuleiten, welche dieser Fähigkeiten derzeit national vorgehalten werden, welche weiteren Fähigkeiten national wünschenswert sind und aufgebaut werden sollten und schließlich die Frage, welche wünschenswerten, derzeit nicht national vorhandenen Fähigkeiten aus (politischen, finanziellen, technologiebasierten) Gründen international zugekauft werden sollten. Dadurch wird die Verfügbarkeit leistungsfähiger, sicherer und vertrauenswürdiger Lösungen am Standort sichergestellt.

2. **Ausbau der deutschen Technologiekompetenz im Design und der Implementierung (hoch-) sicherer Kryptosysteme.** Vier Unterpunkte sind schwerpunktmäßig zu untersuchen:

   a) ITK-Systeme sind zu großen Teilen architektonisch auf Bauelementen bzw. Chipsets nicht-deutscher Hersteller aufgebaut. Auf absehbare Zeit erscheint es aus betriebswirtschaftlichen und auch technologischen Gründen nur mit gebündelten Anstrengungen von Politik und Industrie realisierbar, entsprechende Fertigungsstätten in Deutschland zu etablieren. Davon ausgehend, dass unter dem Blickwinkel der Sicherheit den entsprechenden Schutzmaßnahmen auf Softwareebene im Idealfall stets auf Hardwareebene ein Sicherheitskonzept vorgestellt werden sollte, müssten Schutzmaßnahmen für vitale Infrastrukturen (Netze) bereits auf Ebene der Hardwarearchitektur ansetzen. Risiken be-

EXKURS: GASTBEITRAG DR. SANDRO GAYCKEN, FU BERLIN

ENTNETZUNG ALS WEG AUS DER IT-UNSICHERHEIT

Nach einer gut 40-jährigen Geschichte der IT-Unsicherheit sehen wir gegenwärtig eine neue und weitere Entwicklung des Feldes. Sie ist einer Professionalisierung klassischer und dem Hinzutreten neuer Angreifer geschuldet. Cyberkriminelle werden zu organisierten Cybergangstern mit höheren Zielen als nur Kreditkarten. Und vollkommen neuartige staatliche Cyberkrieger und Cyberspione realisieren verschiedenste geostrategische und wirtschaftspolitische Interessen unterschiedlichster Länder. Durch diesen Wandel in der Landschaft der Angreifer changieren zum einen die Ziele. Neben direkt militärischen Strukturen sind Industriespionage, Wirtschaftssabotage, Manipulation der Börsen und Störung bis Zerstörung kritischer Infrastrukturen plötzlich wesentlich realere und größere Risiken. Es ändert sich aber vor allem auch die Qualität der Unsicherheit, die Höhe der Bedrohung. Denn die neuen und neu entwickelten Angreifer sind wesentlich mächtiger als alle Vorgänger. Sie geben Millionen für einzelne Angriffe aus, arbeiten in großen, organisierten und taktisch geführten Verbänden, operieren mit Nachrichtendiensten und entwickeln – als Standard – Zero Days auf wissenschaftlichem Niveau.

Insbesondere diese hohe Qualität ist es, die als besorgniserregend eingestuft werden muss. Denn sie indiziert einen Sprung in der Offensive, der von der Defensive – der IT-Sicherheit – auch mit besten technischen Standards nicht angemessen beantwortet werden kann. Zumindest nicht, so lange IT-Sicherheit konventionell verstanden wird – als fester Katalog von Adhoc-Maßnahmen, die auf inhärent und strukturell unsichere IT-Landschaften als Sicherheits-Phantasma aufgeklebt werden.

Versteht man IT-Sicherheit jedoch unkonventionell direkt – als das, was getan werden muss, wenn Vertraulichkeit, Integrität und Verfügbarkeit weiterhin gewährleistet werden sollen – kommt man für kritische Bereiche auf einige einfache Paradigmen, mit denen sich das Verhalten von Angreifern und damit die Sicherheit wieder steuern lässt.

Grundlegend sind vier Punkte. Erstens muss Entinformatisierung stattfinden. IT muss überall dort abgebaut und funktional verschlankt werden, wo sie nicht zwingend notwendig ist.

Zweitens muss eine Entnetzung einsetzen. Kritische Wissensbestände oder Steuerungsanlagen gehören nicht an das Internet, denn das Internet wird sich nie beherrschen lassen. Und auch sonst muss vor großen externen Netzwerken wie Clouds gewarnt werden. Diese sind für Angreifer immer attraktiv und oft leicht penetrierbar. Kritische Daten sollten nur in möglichst heterogenen und kleinen, internen und vor direkten wie vor indirekten Infiltrationen geschützten Netzen liegen.

Drittens muss eine harte Micro-IT erforscht, produktisiert und eingesetzt werden, die die chronischen Unsicherheiten der gegenwärtigen Architekturen von vorneherein ausschließt.

Und viertens müssen die Nutzer sicher sensibilisiert und organisiert werden. Nur mit diesen Maßnahmen lassen sich mittelfristig plausible Sicherheitsgewinne gegen die nun vor unserer Tür stehenden starken Angreifer erreichen.

stehen bspw. durch trojanisch gesteuerte, direkte Speicherzugriffe. Da diese Architektur im nationalen oder auch europäischen Alleingang, wie oben illustriert, nur sehr eingeschränkt bis gar nicht beeinflussbar ist, sollten alternative Maßnahmenbündel unter Einbeziehung von Secure-Function-Evaluation-Techniken erarbeitet werden.

Für den Bereich der sicheren Anwendungsausführung sind beispielsweise Kombinationsmöglichkeiten von Endgeräten mit Separation Kernel und hardwarebasierten Sicherheitselementen oder adaptierter, sicherheitsevaluierter Firmware gegeben. Damit kann eine zusätzliche, bedarfsgerechte Verstärkung des Sicherheitsniveaus einer Applikation erfolgen.

Deutschland hat in den nächsten zwei Jahren ein Zeitfenster, diese Technologien, deren Basis bereits vorhanden ist, auszubauen. In Verbindung mit der Einbindung in (massen-) marktfähige Endgeräte und mittels Kombination mit weiteren Technologien können international wettbewerbsfähige Produkte geschaffen werden, welche die sichere Ausführung privatwirtschaftlicher (Bankgeschäfte etc.) und behördlicher Anwendungen (zum Beispiel sichere [mobile] Identifizierung und Authentisierung bei Behördendiensten) erlauben.

b) Anwendungsorientierte Forschung für die rollen- und ebenengerechte Verschlüsselung von Daten auf Feldebene **(selektive datenfeldgranulare Kryptierung)**.

c) Empfohlen wird ferner, forschungsseitig die Frage zu bearbeiten, welche **technologische Nachfolgelösung für FPGAs** (field programmable gateway arrays) sich anbietet. Diese Elemente stellen hardwareseitig ein Kernelement von Kryptographielösungen dar, werden aber derzeit nicht in Deutschland oder der Europäischen Union produziert.

d) Im Bereich **innovativer Kryptoverfahren** sollte eine Studie zur technologischen Leistungs- und Wettbewerbsfähigkeit deutscher Anbieter im internationalen Vergleich erstellt werden, um deutschen Akteuren eine verlässliche Marktsichtung als Ausgangsbasis für eigene Aktivitäten zu gewähren. Darin wären die relevanten Technologien, Akteure (einschließlich Forschungseinrichtungen) und der Stand der Forschung zu erfassen. Ziel wäre es, zu einer verlässlichen Technologiebewertung (einschließlich Produktprognosen) zu gelangen, um entsprechende deutsche Kompetenz langfristig auszubauen. Darauf aufbauen sollte die nachhaltige Überführung der gewonnenen Erkenntnisse in industriell verwertbare, marktfähige Produkte. Begleitend sind geeignete Mechanismen zur Koordinierung der staatlichen und privaten Innovationstätigkeit in diesem Bereich aufzusetzen.

3. Die **Untersuchung potentieller Schwachpunkte im Internet**. Die Zuordnung und Weiterleitung von Datenpaketen im Internet erfolgt weitaus überwiegend via Geräte nichteuropäischer Provenienz. Sofern in der Analyse ein Risiko festgestellt wird, dass durch Fehlfunktionen, technisches Versagen oder Bedienfehler der internationale Datenverkehr kritisch beeinträchtigt werden könnte, wären entsprechende Abhilfsmaßnahmen zu treffen. Diese würden umfassen:

- den Dialog mit den Herstellern der Geräte, um etwaige technische Schwachstellen zu klären,
- die Entwicklung nationaler Lösungen (bzw. aufgrund der Skaleneffekte europäischer Lösungen),

- die über verbindliche Haftungsregeln abgesicherte Verpflichtung von Betreibern kritischer Infrastrukturen, letztere abzusichern. Die Gewährleistung bestimmter Leistungsvereinbarungen kann zum Beispiel durch den Einsatz sicherer deutscher Technologie sichergestellt werden. Gleichzeitig lässt eine Regelung über Haftungsklauseln genügend Spielraum, um auf Ebene der betroffenen Betreiber auch alternativ geeignete Maßnahmen in Betracht zu ziehen.
- Für den Schutz kritischer Infrastrukturen sollte sich die Ergänzung vorhandener Maßnahmen auf die Widerstandsfähigkeit von Netzen, ihre Robustheit und Wiederherstellbarkeit im Schadensfall orientieren.

4. Ausbau der deutschen **Beratungs- und Evaluierungskompetenz** auf dem Gebiet der Hardwaresicherheit. Dies umfasst insbesondere die Systemkompetenz zum Prüfen hardware-, vor allem aber firmwarebasierter Angriffsmöglichkeiten.

5. Ausbau der deutschen **Beratungs- und Evaluierungskompetenz im Bereich der Softwaresicherheit** (einschließlich COTS). Hierzu besteht grundlegender Systematisierungs- und Forschungsbedarf.

6. Bessere internationale Vermarktung erfolgreicher deutscher Projekte, zum Beispiel durch die verstärkte Bereitstellung zielgruppenadäquater Informationen über und Förderung von Internet-Anwendungen, die auf die **sichere Identifizierung über den neuen Personalausweis** (nPA) zurückgreifen. Sowohl die im nPA verwendete Technologie als auch der konzeptionelle Ansatz könnten damit noch stärker ihr Potential ausspielen und Mehrwert für den Nutzer erzeugen. International würde die nPA-Absicherung von Internet-Anwendungen über vereinzelte (Modell-) Projekte hinaus die Attraktivität der gewählten technischen Lösung und damit die Leistungsfähigkeit der deutschen Industrie (Anbieter und Anwender) auf diesem Gebiet unterstreichen.

7. Die Promotorengruppe Sicherheit regt an, die **zwischenstaatliche Zusammenarbeit zur Erhöhung der Sicherheit in Netzen zu verstärken**. Dazu kommen primär multilaterale Foren in Frage.

8. **Ausformulierung einer deutschen Technologieaußenpolitik.**
   Die Entwicklung von IT-gestützten Sicherheitslösungen aus Deutschland findet überwiegend unter Einbeziehung ausländischer Technologiekompetenz oder Technologiekomponenten statt. Umgekehrt ist Deutschland als Exportnation darauf angewiesen, stabile und verlässliche Rahmenbedingungen auf Auslandsmärkten vorzufinden.

   Die Promotorengruppe Sicherheit unterstreicht daher die Dringlichkeit, ressortübergreifend eine stringente Technologieaußenpolitik zur Durchsetzung deutscher Interessen sowohl in den nationalen Märkten der Europäischen Union als auch international zu formulieren. Diese Strategie sollte

   - auf die Schaffung eines fairen, dem Wettbewerb verpflichteten Marktes für sicherheitsrelevante ITK-Produkten und -Lösungen hinwirken;
   - tarifäre und nichttarifäre Handelshemmnisse abbauen;
   - Wettbewerbsvorteile durch die enge Verzahnung der deutschen Botschaften, Kammern und Außenhandelsorganisationen für deutsche Unternehmen sichern;

- ein Instrumentarium zur Lösung wiederkehrender Problemstellungen (etwa im Bereich des geistigen Eigentums, der Marktzugangsbeschränkungen etc.) entwickeln und dabei im permanenten Dialog mit interessierten Kreisen (Industrie, Forschung, Gesellschaft) stehen.

Das spezifische Charakteristikum der deutschen IT-Sicherheitsindustrie ist die starke Zersplitterung der Anbieter- und Forschungslandschaft. Es wird daher empfohlen, konsequent in ressortübergreifender Zusammenarbeit diejenigen **Organisationen zu definieren, deren Kernfähigkeiten als notwendig und national aufbaufähig erachtet werden. Diese Organisationen sind in einem umfassenden strategischen Ansatz in die Lage zu versetzen, international wettbewerbsfähig zu werden**. Eine breit angelegte Förderpolitik allein würde diesem Ziel nicht gerecht: So ist die öffentliche Hand mit einem jährlichen Volumen von ca. 18 Mrd. Euro Beschaffungsvolumen der größte Einkäufer von IT-Dienstleistungen und -produkten in Deutschland (IT-Sicherheit als Teilsegment). Sie kann damit wesentliche Impulse bei der Beschaffung innovativer Produkte und Dienstleistungen setzen, die über die klassischen F&E-Fördermaßnahmen hinausgehen. Dazu zählt nicht allein der eng gefasste Bereich der IT-Sicherheit, sondern insgesamt Anwendungen mit sicherheitsrelevanten Komponenten.

Derartige Maßnahmen sind nicht allein Industrie-, sondern vorrangig **Sicherheitspolitik**. Sie sichern nationale Souveränität und damit nicht zuletzt auch **Handlungsfähigkeit** und **Mitsprachemöglichkeiten auf internationaler Ebene**. Nicht zuletzt dürfte eine vergaberechtskonforme Ausgestaltung sicherheitsrelevanter Beschaffungspolitik deutscher Kernkompetenzen die Auswirkungen von (vermuteten, bewusst eingebauten) Sicherheitslücken nicht-deutscher Lösungen wesentlich verringern. »Stärken stärken« muss die handlungsbestimmende Maxime sein – bei Ausschreibungen, Forschungsförderung und der Unterstützung von Kooperationen. Ziel ist dabei, nicht nur Technologie aus Deutschland, sondern deutsche Technologie im Sinne der Beherrschung strategischer Teile der Wertschöpfungskette durch deutsche Akteure auszubauen.

Die Promotorengruppe Sicherheit wird dazu in Abstimmung mit den zuständigen Ressorts Handlungsempfehlungen mit detaillierten Umsetzungsmaßnahmen vorschlagen.

4 ZUKUNFTSINITIATIVEN

4.1 Zukunftsinitiative Sicheres Cloud Computing

4.1.1 Ausgangslage

Die in den Massenmedien inflationäre Verwendung des Begriffs Cloud Computing hat in Teilen zu einer begrifflichen Unschärfe des Bedeutungsinhaltes geführt. Einige der Fragen, die Cloud-spezifisch thematisiert werden (Zugang zu Daten, Datensicherheit usw.) sind bspw. kein reines Cloud-Phänomen, sondern ein bereits im Vorfeld zu betrachtender IT-Sicherheits-Prozess, der durch die Cloud teils verlängert, teils ausdifferenziert wird. Eine homogene Cloud-Definition ist ferner schwer möglich: Dazu ist die Anwendungspraxis (Datenauslagerung oder zusätzliche Datenverarbeitungsprozesse in der Cloud bzw. Dienstleistungen aus der Cloud) zu breit ausgefächert, national unterschiedlich weit vorangeschritten und nach Branche resp. Einzelanwender zu unterscheiden.

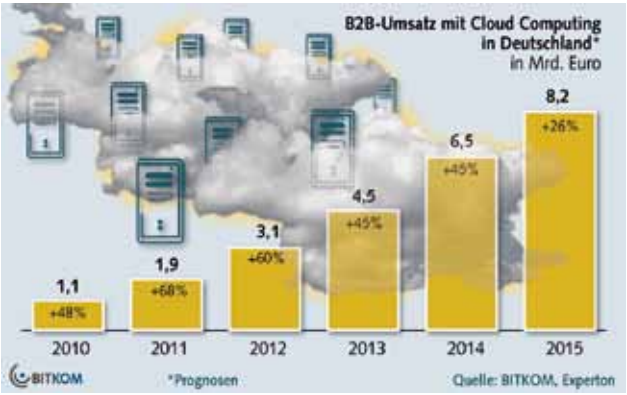


Abbildung 13: Rechnen mit der Wolke (Quelle: BITKOM)

Die in Fachkreisen konstatierte Heterogenität der strukturellen und prozessualen Cloud-Betrachtungen führt dazu, dass eine uniforme Sicherheitsanalyse und Abgabe entsprechender Handlungsempfehlungen ins Leere laufen müssten. Vergleichbar der Situation bei Embedded Systems muss eine Sicherheitsanalyse zudem die gesamte Prozesskette berücksichtigen und stets einem die Gesamtarchitektur berücksichtigenden Ansatz folgen, um Interdependenzen einzelner sicherheitskritischer Komponenten – auf den Einzelfall zugeschnitten – untersuchen zu können. Gleichwohl stechen einzelne Punkte heraus, bei denen die technologische Kompetenzbasis in Deutschland auszubauen ist, um zum gewünschten Zukunftsszenario 2020 »Sichere Cloud designed by Germany« zu gelangen.

Sicherheit ist hier begrifflich zweigeteilt: Sicherheit in der Cloud und Sicherheit durch die Cloud. Bisher beschäftigen sich die meisten Expertengremien mit der Frage, wie die Cloud, die in ihr

gespeicherten Daten bzw. laufenden Programme sicher gemacht werden können. Diese Betrachtung sollte ergänzt werden: Gegenüber herkömmlichen Datenzugriffs-, -speicher- und –verarbeitungsmechanismen (meist redundant ausgelegt) bietet die Cloud sicherheitsfördernde Möglichkeiten, Dateien flexibel skalierbar und vor allem physisch getrennt abzulegen. Diese Ablage und Verarbeitung auf mehreren Servern kann so erfolgen, dass selbst die Manipulation eines einzigen Servers nicht automatisch die Kompromittierung aller Server und der dort abgelegten Datensätze zur Folge hat. Konkret: Selbst im Falle eines erfolgreichen Angriffs bzw. unauthorisierten Datenzugriffs sind zwar einzelne Daten kompromittiert, (wirtschaftlich) nutzbare Informationen können jedoch daraus nicht generiert werden. Hier zeigt sich eine intrinsische Widersprüchlichkeit der Sicherheit bei und von Informations- und Kommunikationssystemen. Dem Wunsch nach Datensparsamkeit und dem Schutz vor unerlaubten Zugriffen auf Informationen einer Organisation oder eines Individuums steht die Erfordernis der redundanten Datenablage zum Schutz vor Datenverlust und zur Erhöhung der Ausfallsicherheit entgegen.

4.1.2 Übergreifende Handlungsempfehlungen

4.1.2.1 FORSCHUNG UND ENTWICKLUNG

1. Forschung zu **Datenverschlüsselung auf Feld- / Datensatzebene.**

Begründung: Um zu einer werthaltigeren Cloud zu gelangen – von der Datenspeicherung hin zur sicheren Diensteerbringung – muss der rollen- und ebenengerechte Zugang zu Teilmengen von Datensätzen, deren Verarbeitung und wiederum rollen-, ebenengerechte, personenadäquate und physisch korrekte Ausgabe technologisch ermöglicht werden. Erst die Existenz derartiger Mechanismen würde beispielsweise im deutschen Kontext die rechtskonforme Erstellung von behördlichen Clouds ermöglichen.

Bisherige Verschlüsselungsverfahren, die Datensätze in der Regel komplett verschlüsseln, würden eine entsprechende Business Intelligence entweder verhindern oder müssten zur Ermöglichung derselben (kurzfristig) aufgehoben werden. Zudem könnte die Datenverschlüsselung auf Feld- bzw. Datensatzebene in speziellen Einsatzszenarien, bei denen eine breitbandige Übertragung verschlüsselter Komplettdatensätze nicht gewünscht oder technologisch nicht möglich ist, entsprechende Nutzererfordernisse beantworten.

Geeignete Verschlüsselungsverfahren, zum Beispiel homomorphe Verschlüsselung, sind methodisch zu erforschen und Marktteilnehmern zur Verfügung zu stellen, um einen wirklichen Mehrwert für Nutzer von Cloud-Diensten zu generieren und Cloud Computing nicht auf das alleinige Auslagern von Daten zu beschränken.

2. Bereitstellung eines **Third-Party-Mehrwertanwendungs-Layers**
Begründung: Die Promotorengruppe Sicherheit geht davon aus, dass der quantitative Infrastruktur-Vorsprung ausländischer – primär US-amerikanischer – Cloud-Anbieter durch deutsche Firmen kurz- und mittelfristig nicht aufgeholt werden kann. Gleichzeitig werden kostenbewußte Cloud-Anwender schwerlich zur Nutzung einer potentiell höherpreisigen, »deutschen« Cloud mit erweiterten Sicherheitsmerkmalen bewegt werden können, sondern sie werden ihr Handeln an aus ihrer Sicht ökonomischen Kriterien orientieren.

Teilelement Sicherheit. Chancen für deutsche Anbieter bestehen darin, Sicherheit als gesamtarchitektonisch integrierbares Angebot, welches on demand modular an marktverfügbare Cloud-Angebote gekoppelt werden kann, zu definieren. Alternative Geschäftsansätze im Sinne eines positiv konnotierten Regulierungsexports (insbesondere in Punkto Datenschutz und –sicherheit) aus Deutschland heraus dürften im Sinne des international dominanten »best cost«-Paradigmas schwerlich zu plazieren sein. Die Schaffung einer stabilen, modular erweiterbaren Sicherheits-Zwischenschicht (Middleware) im jeweiligen IT-Gesamtsystem des Unternehmens böte dagegen auch kleinen und mittleren Unternehmen aus Deutschland die Chance, Marktnischen mit deutscher Kompetenz innovativ zu besetzen.

Dieser Ansatz setzt die Existenz einer Sicherheitsmetrik voraus und entbindet Unternehmen nicht von der grundsätzlichen Befassung mit ihrer internen IT-Sicherheitsarchitektur (was soll, was kann in die Cloud ausgelagert werden).

Teilelement Compliance. In stärker regulierten Branchen (zum Beispiel Bankwesen, pharmazeutische Industrie) steht der kostengünstigen Auslagerung von Geschäftsprozessen bzw. dem nachfrageorientierten Bezug von Cloud-Computing-Dienstleistungen sehr häufig ein national und materiell ausdifferenziertes Regelungswerk zum Umgang mit Daten gegenüber. Dadurch wird die unternehmensweite Vereinheitlichung von Geschäftsprozessen deutlich verlangsamt; Skaleneffekte und damit die Attraktivität von Cloud Computing nehmen in diesen sicherheitssensiblen Branchen ab. Anbieter, die sich in der o. a. Zwischenschicht als Compliance-Konnektor (im Sinne eines »Übersetzers« zur Herstellung der regulatorischen Regelkonformität bei Datenübergabe, -transport und –verarbeitung) etablieren, könnten ihr entsprechendes Prozesswissen international erfolgreich in der jeweiligen Branche vermarkten.

Die Herausbildung entsprechender Geschäftsmodelle kann durch F&E-Maßnahmen, die auf einen sehr engen Dialog mit den Anwenderbranchen abstellen, unterstützt und beschleunigt werden. Dazu soll eine Plattform aufgesetzt werden, die dem Wissensaustausch und der Lösungsentwicklung dient, etwaigen weiteren F&E-Bedarf identifiziert und die Konsortialbildung interessierter Unternehmen durch deren Vernetzung unterstützt (vgl. vorliegende Empfehlungen der Promotorengruppe Sicherheit).

3. **Schaffung eines nationalen Testbeds »Sicheres Cloud Computing«**
Begründung: Vor dem bekannten Hintergrund der Interdependenz komplexer Systeme, der Sensibilität bestimmter Anwender (-Branchen) für Sicherheit sowie dem steigenden Angriffsdruck auf IT-Systeme (bis hin zu Cyberwar-Szenarien) ist es erforderlich, Cloud-Architekturen in einem nationalen, virtuellen Cloud-Testbed verschiedenen Angriffsszenarien zu unterziehen. Damit

soll bereits vor der Vermarktung von Cloud-Angeboten deren Widerstandsfähigkeit gegen sicherheitsrelevante externe Angriffe oder deren Missbrauch, zum Beispiel im Rahmen von Bot-Netzen, geprüft und erhöht werden. Mittelfristig wird dadurch ein qualitativer Sicherheitsgewinn von Cloud-Angeboten deutscher Firmen erzielt.

4. Schaffung eines Siegels für nationale, sichere Anbieter
Begründung: Als wesentlicher technologischer Wettbewerbsvorteil wird die Erfahrung deutscher Anbieter mit Themen wie Datensicherheit und Datenschutz angesehen. Anbieter, die einen bestimmten, noch zu definierenden Kriterienkatalog in diesen beiden Kategorien erfüllen (einschließlich Passieren des oben aufgeführten Cloud-Testbeds), sollen auf Antrag ein entsprechendes Siegel erhalten. Das Siegel bezieht sich auf eine technologieoffene und prozessfokussierte Zertifizierung und zielt damit auf die Transformation des »Produkts Cloud« zu einer integrierten Technologielösung. Diese sollte transparent sein sowie interoperable Schnittstellen zu sicherheitsrelevanten Middleware-Lösungen anbieten. Damit wird eine Differenzierungsmöglichkeit für deutsche Technologie im internationalen Wettbewerb geschaffen.

4.1.2.2 REGULIERUNG

Wie einzelne Experten hervorheben, fehlt im Bereich Security im Gegensatz zu Safety, die «messbar« und validierbar ist, eine vergleichbare Metrik. Diese ist allerdings Voraussetzung für stabile Kalkulationen von Risiko und Eintrittswahrscheinlichkeit sicherheitsrelevanter Ereignisse, für die Erarbeitung von Haftungsregelungen, für die exakte Verantwortungszuteilung bei Cloud-Diensten sowie insgesamt die Schaffung von Rechtssicherheit bei der Auslagerung von Datenverarbeitung und Geschäftsprozessen in die Cloud. Die Promotorengruppe Sicherheit regt daher an, seitens der zuständigen Ressorts Forschung zur Realisierbarkeit von »Security Economics« zu unterstützen.

Regulierungsseitige Positivaspekte, die von deutschen Anbietern international vermarktet werden können, sollten zudem über geeignete Mechanismen mit Vermarktungs- und Technologieaspekten zusammengeführt werden.

4.1.2.3 VERMARKTUNG

Ausgehend von der Erkenntnis der beiden vorhergehenden Abschnitte, dass Sicherheit als Geschäftsmodell auch im Bereich Cloud Computing tragfähig ist und deutsche Anbieter hierbei besondere Stärken aufweisen, sollten Mechanismen entwickelt werden, die deutsche Kompetenz international wettbewerbsfähig zu vermarkten. Dazu gehören u. a.:

- Die Positionierung von sicherem Cloud Computing (deutscher Anbieter bzw. auf der Basis in Deutschland entwickelter und auf den Markt gebrachter Lösungen) als Sicherheitschance – und nicht als perzipierte Belastung – für die Anwender;

- Die Erarbeitung bzw. der Ausbau von technischen Spezifizierungen und Schutzprofilen (BSI in Zusammenarbeit mit Anwendern und Anbietern);

- Die Erarbeitung spezifischer Branchenanforderungen, zum Beispiel Skalierbarkeit im Sinne einer elastischen Cloud;

- Die Erarbeitung von international gangbaren Musterverträgen und die Bündelung von Angebots- und Nachfragemarktmacht gegenüber international dominanten Anbietern mit dem Ziel, auch bei Angebot und Nutzung von Sicherheitseigenschaften zu relevanten Skaleneffekten zu gelangen.

4.2 Zukunftsinitiative Sichere Embedded Systems

4.2.1 Ausgangslage

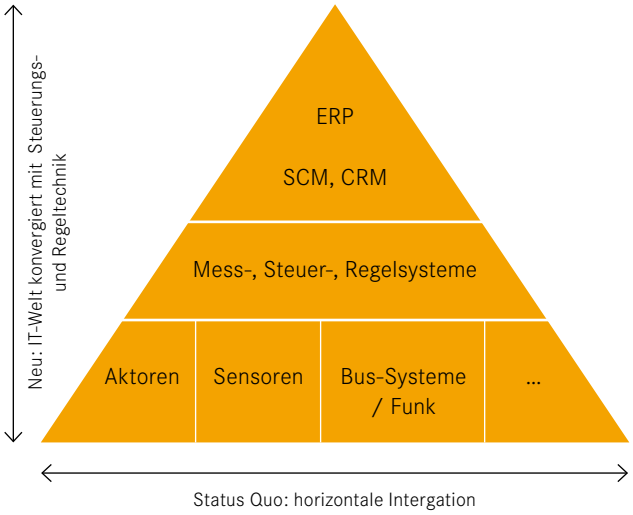


Abbildung 14: Embedded Systems in der ITK, Beispiel Smart Factory / Automatisierungspyramide

Nicht nur die Gewährleistung der Sicherheit von, sondern auch die Sicherheit durch Embedded Systems (ES) dürfte in den kommenden Jahren zu einer Bewährungsprobe werden. Dies gilt sowohl für »unsichtbar« verbaute elektronische Mess-, Steuer- und Regelsysteme (Embedded Systems ohne zwingende externe Netzanbindung) als auch für die sog. Cyber-Physical Systems (CPS als Pattern, dass eine logische Vernetzung zwischen Komponenten auf Feldebenen - Sensoren, Aktoren und ES - mit Anwendungssoftware entweder dynamisch oder hierarchisch umschreibt). Drei ursächliche Trends wurden in diesem Kontext identifiziert.

1. Die Tendenz, aus Kosten- und Performanzgründen im Umfeld von Embedded Systems auf handelsübliche IT und Elektronik zu setzen (COTS), führt möglicherweise durch die nicht in letzter Konsequenz mögliche Sicherheitsüberprüfbarkeit verbauter Systeme zu ungewollten Lücken im Schutzkonzept – sowie zur Abhängigkeit von einigen wenigen Herstellern.

2. In industriellen Großanlagen, Maschinen und weiteren Investitionsgütern, aber auch in fliegenden und schwimmenden Systemen sind Embedded Systems integriert, deren Funktionalität über die Laufzeit von zuweilen mehreren Jahrzehnten nicht abnimmt. Sie sind hingegen möglichen Sicherheitslücken durch Änderungen im IT-Gesamtsystem ausgesetzt, deren Existenz zum Zeitpunkt der Konzeption nicht vorhersehbar war. Zu untersuchen wäre, inwiefern ein optimiertes Änderungs- und Obsoleszenzmanagement planerisch ex ante im Gesamtsystem stärker als bisher unter dem Blickwinkel der Sicherheit bedacht werden kann.

3. Es wird von der Grundüberzeugung ausgegangen, dass die ES-Märkte der Zukunft noch weniger als bisher von einer Produkt-, sondern vielmehr von einer Lösungslogik dominiert werden. Führende Hersteller werden diejenigen Anbieter sein, denen es gelingt, wesentliche Teile der Wertschöpfungskette (als erfolgreiches Beispiel mögen bekannte Consumer-Electronics-Produkte amerikanischer Telefon- und Tablet-PC-Hersteller dienen) – dies schließt Sicherheit als Funktion ausdrücklich ein! – zu beherrschen. Sicherheit wird nach Expertenmeinung nur dann nachhaltig im Markt verankert werden, wenn die Beherrschung von Wertschöpfungsketten nicht an die Kapselung von Systemen gekoppelt wird (»Security by Obscurity« als illustrative Überhöhung). Kosten- und Effizienzgründe sowie der Wunsch nach offenen, modular aufgebautem ES-Systemkomplexen der Zukunft werden insofern das Verlangen der Anwender nach nicht-proprietären, sondern durch technologische Exzellenz und deren Sicherheit überzeugenden Systemen determinieren.

4.2.2 Kompetenzen und Handlungsbedarf

Der Einsatz von Embedded Systems findet in Deutschland industrieübergreifend statt: Vom Maschinen- und Anlagenbau über die Automobilindustrie bis hin zu Herstellern einzelner Elektronikkomponenten. Damit ist der Kern der industriellen Wertschöpfung in Deutschland einschließlich mehrerer Millionen hochqualifizierter Beschäftigter zunehmend in Forschung, Herstellung und den weltweiten Vertrieb von Produkten eingebunden, deren funktionale Sicherheit und auch deren Funktionalitäten zur Gewährleistung von Sicherheit in Gesamtsystemen häufig untrennbar miteinander verbunden sind. Untersuchungen und Studien zu diesem und benachbarten Themenfeldern, wie beispielsweise von der Promotorengruppe Kommunikation und der Acatech (»Industrie 4.0«) durchgeführt, sind wesentlich für die Sicherung industrieller Kernfähigkeiten am Standort Deutschland.

Dennoch nimmt Sicherheit zumindest in Produktionsprozessen über die funktionale Sicherheit von Komponenten hinaus bisher eine sekundäre Rolle ein, obwohl durch die (internationale) Auslagerung industrieller Teilprozesse einige Fragen aufgeworfen werden:

- Wie kann das (IT-) Sicherheitswissen aus der konventionellen (Office-IT-) Welt in die Welt der Embedded Systems überführt werden? Hierbei ist zu beachten, dass im industriellen – sicherheitskritischen – Umfeld oft höhere Anforderungen an die Funktionssicherheit der Steuer- und Regelsysteme, deren Geschwindigkeit (Echtzeiterfordernis bei sicherheitskritischer Automatisierung und Steuerung), Integrität und Manipulationssicherheit gestellt werden, als dies im herkömmlichen Office-Umfeld erforderlich ist.

Es stellt sich ferner die Frage, welche gemeinsame Sprache, welche gemeinsamen Benennungen dafür erforderlich sind.

- Wie kann die Sensibilisierung der Anwender für Security-Themen im ES-Kontext erfolgen, insbesondere mit Blick auf unauthorisierte Zugriffe aus dem System heraus bzw. durch Dritte? Hierbei kommt aus Sicht der Promotorengruppe dem Staat eine wesentliche Rolle zu. So wird beispielsweise mit der Einführung intelligenter Stromzähler (Smart Metering als Teil eines Smart Grid) erstmals verpflichtend die Verwendung von ITK-Systemen außerhalb des hoheitlichen Bereichs für den Endnutzer festgeschrieben. Es erscheint daher zwingend, dass relevante Sicherheitsfragen vorab und umfassend in der Zusammenarbeit mit Industrie und Forschung geklärt werden.

- Welche Geschäftsmodelle lassen sich in dem Bereich entwickeln? So ist im Bereich der Fernwartung, der Fernwirkung und der Ferndiagnose ein Marktpotential für den Maschinenbau zu erwarten, das die Notwendigkeit der Security-Berücksichtigung deutlich vor Augen führt. Während sich die Möglichkeiten und Anwendungsbereiche der Fernwartung, -wirkung und -diagnose vervielfacht haben, sind für deren Einsatz spezifisches IT-Know-How oder komplexe Konfigurationswerkzeuge erforderlich. Bei der zunehmenden Systemkomplexität und -differenzierung werden einfach handhabbare Tools erforderlich sein und sind durch Fortbildungsmaßnahmen der Fachtechniker zu begleiten.

Eine Impulssetzung für Embedded Systems unter dem Blickwinkel der Sicherheit ist bei der Heterogenität des Themenfeldes nur im Zusammenspiel von Herstellern und Anwendern bei gleichzeitiger innovationspolitischer Begleitung durch die Politik möglich. Dabei empfiehlt sich ein prozess- oder szenarioorientierter Ansatz eher als eine generische Betrachtung, die zwangsläufig nur einzelne Punkte umfassen kann.

4.2.3 Übergreifende Handlungsempfehlungen

1. Ausbau der nationalen Kompetenzbildung
Embedded Systems mit dem Schwerpunkt Safety und Security (insbesondere für vertikal und horizontal vernetzte Systeme)

Begründung. Die Promotorengruppe stimmt dahingehend überein, dass in Deutschland signifikante ES-Entwicklungskompetenz vorhanden ist. Die Kompetenzen sind allerdings stark (nach Branchen, Anwendungsfällen) segmentiert; eine übergreifende Vernetzung findet bisher selten statt.

Zudem ist es mit Blick auf den zunehmenden Schutz- und Sicherheitsbedarf von Embedded Systems notwendig, auf der Basis einer zu erstellenden Sicherheitsmetrik verbindlich messbare Kriterien für Systemsicherheit im ES-Kontext zu erarbeiten. Arbeiten dazu finden beispielsweise in den Kompetenzzentren Karlsruhe, Darmstadt und Saarbrücken statt.

Ausgewählte Embedded-Systems sollten ferner – einschließlich der sicherheitsrelevanten Komponenten – in einem Testbed einer Erprobung auf Angriffe unterzogen werden. Dabei ist die Verlässlichkeit und Widerstandsfähigkeit der gesamten ES-Funktionskette zu betrachten, nicht nur die der klassisch bisher einer Einzelprüfung (meist nur im Sinne von Produktsicherheit) unterzogenen ES-Teilkomponenten. Die für dieses Forschungsvorhaben benötigten Ressourcen dürften angesichts der Komplexität der Aufgabe nicht unerheblich sein. Daher sollte die entsprechende Allokation gebündelt erfolgen, um Expertise themenzentriert und räumlich konzentriert zusammenzuführen.

Besonderes Augenmerk sollte der Herausbildung von Systemdesign-Fähigkeiten beim wissenschaftlichen Nachwuchs gelten. Insofern ist ein interdisziplinärer Aus- und Fortbildungsansatz (Informatik mit Schwerpunkt Sicherheit Eingebetteter Systeme / IT-Sicherheit, Wirtschaftswissenschaften) erstrebenswert.

2. Identifikation sicherheitsrelevanter ES-Wertschöpfungsketten
Begründung: Um eine rasche Überführung technologischer Erkenntnisse in die Praxis zu erleichtern, empfehlen die Promotoren, parallel zum Aufbau der entsprechenden Kompetenzzentren eine Untersuchung vorzunehmen, welche in Deutschland (und in einem zweiten Schritt europaweit / international) besonders sicherheitssensiblen ES-Anwendungsfelder existieren. Die dergestalt identifizierten Anwendungsfelder (in Einzelfällen vermutlich auch Branchen) sollten in einer engen Zusammenarbeit von Anbietern und Anwendern, universitärer und außeruniversitärer Forschung daraufhin überprüft werden, inwiefern (in der Sicherheit bedarfsgerecht skalierbare) Embedded Systems in den entsprechenden Prozessketten dergestalt integriert werden können, dass eine gegenseitige sichere Identifizierung, Authentifizierung und Validierung von Einzelkomponenten zur Sicherheit des Gesamtsystems beitragen kann. Eine allgemeine »Security-Norm« existiert bisher nicht.

Eine besondere Rolle kommt der Standardisierung zu. Um die Vervielfältigung möglicher Sicherheitslücken kritischer Systeme bzw. der Funktionsfähigkeit sicherheitsschaffender Systeme zu minimieren, sollten weitflächig standardisierte, in ihren Varianten nicht allzu stark ausdifferenzierte Teilsysteme verwendet werden. Um die Kommunikation und Interoperabilität von Komponenten und Ebenen in zukünftigen

BEISPIEL: »SMART FACTORY«

Die Investitionsgüterindustrie, hier insbesondere der Maschinen- und Anlagenbau, ist mit mehr als 910.000 Beschäftigten in Deutschland ein zentraler Wachstumsmotor. Der zunehmenden internationalen Konkurrenz können Unternehmen aus Deutschland in der Regel nicht mit einer Niedrigpreisstrategie, sondern nur mit hoher Innovationskraft und nachhaltiger Präsenz auf internationalen Märkten begegnen. Dazu sind die industriellen Wertschöpfungsketten weiter zu flexibilisieren, zunehmend aber auch die Maschinen und Fertigungsanlagen selber. Damit kann der Forderung des Kunden nach individuellen Konfigurationsmöglichkeiten und kurzen Lieferfristen unter Berücksichtigung wirtschaftlicher Skaleneffekte in der Massenproduktion begegnet werden.

Flexibilität bedeutet dabei:

- Externe Öffnung des Unternehmens und Anpassung seiner Wertschöpfungstiefe in Abhängigkeit vom jeweiligen Geschäftsmodell und
- Flexibilisierung des eigenen Produktionssystems.

Die Lösung: ITK-gestützte Smart Factories zeichnen sich durch die Fähigkeit aus, agil auf Kundenbedürfnisse eingehen zu können. Dazu wird auf Komponentenebene (horizontal) als auch schichtenübergreifend (zum Beispiel ERP-System, CRM, SCM usw.) die informationstechnische Vernetzung ausgebaut und Flexibilität bei Steuerung und Produktion geschaffen.

CPS-Modellen (vertikale und horizontale Kommunikation von Komponenten und logischen Schichten) zu verbessern, dürfen Fehler der Vergangenheit – erwähnt sei zum Beispiel die Vielzahl von Feldbus-Varianten – nicht wiederholt werden (zum Beispiel bei der Anzahl der Ethernet-Varianten). Sichere Kommunikationsstandards müssen nicht zuletzt bei der verstärkten Hinwendung zum Industrie-4.0-Paradigma (Unternehmenssteuerung in Echtzeit, Flexibilität in der Wertschöpfungskette einschließlich systemischer Interoperabilität, adaptive Produktionssysteme), sichere M2M-Kommunikation inbegriffen, oberste Priorität haben.

Flankierend sind Standardisierungsaktivitäten (sowohl Industriestandards als auch formale Standardisierungsgremien) zu unterstützen, um deutscher Spitzentechnologie eine herausragende Position auf dem Weltmarkt zu sichern. Dabei ist auf die internationale Kompatibilität von regulatorischen Maßnahmen zu achten, die einen deutschen Vorlauf jedoch nicht ausschließen. Die im BITKOM vertretene ITK-Industrie plant begleitend dazu eine umfassende Analyse von Safety- und Security-relevanten Normen und Standards – Schwerpunkt CPS – mit Blick auf verschiedene Branchenanforderungen.

Die Notwendigkeit der Arbeit an Normen und Standards sollte auch an den deutschen Hochschulen und (technischen) Universitäten stärker ins Bewusstsein gerückt werden. Hierbei könnte durch die verstärkte Einbindung der Hochschulen – ebenso wie die Unterstützung der mittelständischen Wirtschaft durch die öffentliche Hand – in die nationale und internationale Gremienarbeit schon früh der wissenschaftliche und industrielle Nachwuchs an dieses wichtige Thema herangeführt werden.

3. **Akzeptanzmanagement:** Parallel zu technologischen F&E-Aktivitäten und entsprechenden Begleitmaßnahmen (einschließlich der Verankerung von sicherheitsrelevanter ES-Entwicklungskompetenz in Deutschland) wird empfohlen, eine Untersuchung zum gesellschaftlichen Akzeptanzmanagement (einschließlich Anwendergruppen) von Sicherheit in, von und durch Embedded Systems zu beginnen.

   Begründung: In zahlreichen Expertengesprächen wurde festgestellt, dass trotz medialer und faktisch auch wahrnehmbarer Bedrohungslagen von Embedded Systems (Beispiel »Stuxnet«) die Bereitschaft der Anwender, in Sicherheit zu investieren, sehr überschaubar ist. Sofern Sicherheit als ergänzende »Option« angeboten wird, scheint in Einzelfällen mit einer gewissen Fatalitätsmentalität gehandelt zu werden, welche volkswirtschaftlich inakzeptabel ist. Es ist aus diesem Grund unumgänglich, neben der notwendigen Entwicklung zukunftsträchtiger CPS-Geschäftsmodelle auch Sicherheit mit einem besonderen Schwerpunkt Datenschutz von Anbeginn mitzudenken. Dies betrifft insbesondere die Schnittmenge personenbeziehbarer (physischer, virtualisierter, virtueller) Daten mit objektbezogenen Daten. Ein einheitlicher »Werkzeugkasten« für den Ausbau der Sicherheit im CPS-Bereich wäre aufgrund der Komplexität der Einsatzszenarien wenig realistisch. Umso wichtiger scheint es, beim Aufbau von CPS Datenschutzaspekte (da zunehmend in Geschäftsmodellen relevant) architektonisch zu berücksichtigen, um die gesellschaftliche Akzeptanz zu fördern und auch weiterhin wettbewerbsfähige Lösungen made in Germany auf dem Weltmarkt anbieten zu können.

   Sicherheit von und durch Embedded Systems sollte kommunikativ positiv konnotiert werden, um Anwender entsprechend zu sensibilisieren. Zur Unterstützung der Anwender sollte, beginnend im Safety-Bereich und hinführend zur Security, eine Vereinheitlichung der Begriffs- und Definitionsbasis erarbeitet und in einer allgemein zugänglichen Datenbank abgelegt werden. Damit kann eine übermäßige Abhängigkeit der Anwender von proprietären Herstellerstandards verringert werden. Zudem würde es erleichtert, unabhängig von Herstellerangaben zu einer soliden Risikobeurteilung von Komponenten gelangen zu können.

   Staatliche Regulierung durch Vorschriften und Gebote schließt sich hier – von einzelnen ohnehin regulierten Branchen abgesehen – aufgrund des Detaillierungsgrades der Materie aus. Gleichwohl böte sich die Chance, auf der Basis eines engen Dialogs mit Anwendern und Anbietern bestimmte Schutzziele zu benennen und staatlicherseits als wichtig erachtete Sicherheitserfordernisse proaktiv politisch zu unterstützen (dies schließt die Unterstützung des Mittelstands bei der Einführung von Sicherheitslösungen ein), um die Wettbewerbsfähigkeit der deutschen Wirtschaft – einschließlich der Widerstandsfähigkeit gegen externe Angriffe – auszubauen.

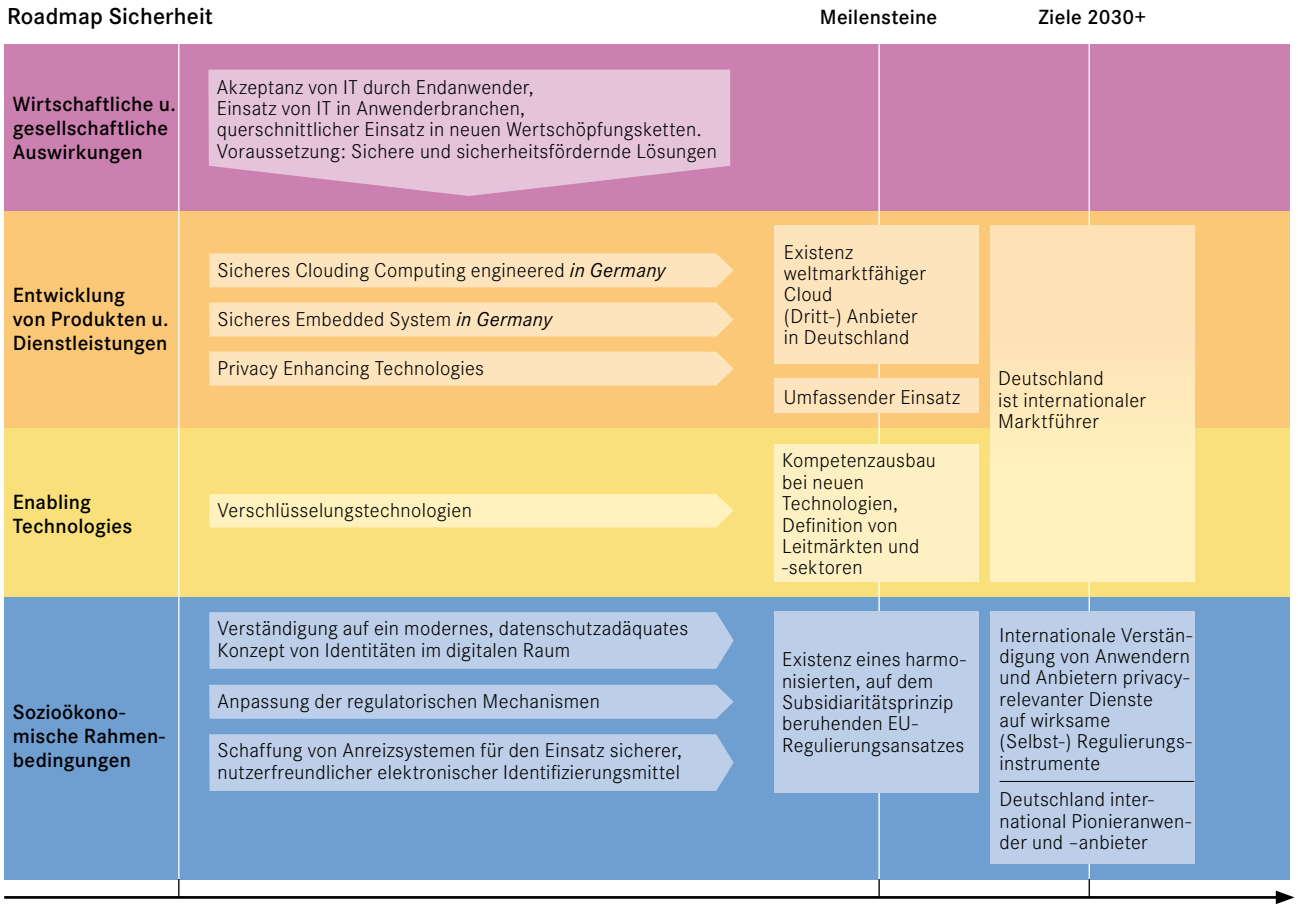
Als Startpunkt sollte in einer als sicherheitsrelevant identifizierten Branche (bspw. Maschinen- und Anlagenbau, Energieinfrastrukturbetreiber gemeinsam mit der ITK-Industrie) ein Demonstrator aufgebaut werden. Dieser würde die Interoperabilität auf Komponentenebene in einem ausgewählten CPS-Szenario nachweisen. Dabei wäre auf folgende Punkte besonderes Augenmerk zu richten:

- Marktrelevanz
- Skalierbarkeit
- Integrationsfähigkeit in ganzheitliche Sicherheitsarchitekturen

bei gleichzeitiger Berücksichtigung der szenariospezifischen Normen und Standards.

Eine wichtige Rolle kommt nach Auffassung der Promotorengruppe Sicherheit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu, das sowohl durch Zertifizierungsmaßnahmen im ES-Bereich (Stichwort Smart Metering) als auch durch seine Entwicklungsexpertise maßgeblich zur Fortentwicklung des Themas beitragen kann.

5 ROADMAP


Roadmap Sicherheit
Meilensteine
Ziele 2030+
Wirtschaftliche u. gesellschaftliche Auswirkungen
Akzeptanz von IT durch Endanwender, Einsatz von IT in Anwenderbranchen, querschnittlicher Einsatz in neuen Wertschöpfungsketten. Voraussetzung: Sichere und sicherheitsfördernde Lösungen
Entwicklung von Produkten u. Dienstleistungen
Sicheres Clouding Computing engineered *in Germany*
Sicheres Embedded System *in Germany*
Privacy Enhancing Technologies
Existenz weltmarktfähiger Cloud (Dritt-) Anbieter in Deutschland
Umfassender Einsatz
Deutschland ist internationaler Marktführer
Enabling Technologies
Verschlüsselungstechnologien
Kompetenzausbau bei neuen Technologien, Definition von Leitmärkten und -sektoren
Sozioökonomische Rahmenbedingungen
Verständigung auf ein modernes, datenschutzadäquates Konzept von Identitäten im digitalen Raum
Anpassung der regulatorischen Mechanismen
Schaffung von Anreizsystemen für den Einsatz sicherer, nutzerfreundlicher elektronischer Identifizierungsmittel
Existenz eines harmonisierten, auf dem Subsidiaritätsprinzip beruhenden EU-Regulierungsansatzes
Internationale Verständigung von Anwendern und Anbietern privacy-relevanter Dienste auf wirksame (Selbst-) Regulierungsinstrumente
Deutschland international Pionieranwender und -anbieter

6 DANKSAGUNG

Die Promotorengruppe Sicherheit bedankt sich bei den nachstehenden Firmen und Organisationen, die durch die Entsendung von Experten in Workshops zu den Themen Sichere Identitäten, Sicheres Cloud Computing und Embedded Security die Redaktion des Dokuments unterstützten bzw. die durch ihren fachlichen Rat in Einzelgesprächen wertvollen Input gaben (in alphabetischer Reihenfolge).

Prof. Dr.-Ing. Jürgen Beyerer
(Karlsruhe Institute of Technology / Fraunhofer IOSB)
und Mitarbeiter

Michael Bobrowski
(Verbraucherzentrale Bundesverband)

Prof. Dr.-Ing. Rainer Böhme
(Universität Münster)

Thomas Brückner
(Bundesverband der Pharmazeutischen Industrie)

André Dornbusch
(Bundeskriminalamt)

Ralf Förster
(KHS)

Florian Glatzner
(Verbraucherzentrale Bundesverband)

Dr. Sandro Gaycken
(FU Berlin)

Stephan Gerhager
(E.ON)

Dr. Bernd Grobauer
(Siemens)

Dr. Waldemar Grudzien
(Bundesverband deutscher Banken),

Sven Gundlach
(BWI)

Dr. Boris Hemkemeier
(Commerzbank),

Sven Herrmann
(BMBF)

Harald Hönninger
(Bosch)

Dr. Detlef Houdeau
(Infineon)

Klaus Julisch
(IBM)

Eva-Maria Kirschsieper
(Facebook)

Dr. Lutz Jänicke
(Innominate)

Dr. Wolfgang Klasen
(Siemens)

Bernd König
(BWI)

Bernd Kowalski
(BSI)

Ulrich Kunitz
(Deutsche Bank)

Christoph Lauer
(ehem. Mitglied im Bundesvorstand der Piratenpartei)

Holger Lieb
(Daimler)

Volkmar Lotz
(SAP)

Olivier Mari
(EADS Cassidian)

Herr Mörl
(IT-Watch)

Prof. Dr. Jörn Müller-Quade
(Karlsruhe Institute of Technology)

Dr. Wolf Osthaus
(1&1 Internet AG)

Dr. Dr. Michael Paulitsch
(EADS)

Prof. Dr. Alexander Roßnagel
(Universität Kassel)

Dr. Heiko Roßnagel
(Fraunhofer IAO)

Prof. Dr. Volker Roth
(FU Berlin)

Ingo Ruhmann
(BMBF)

Prof. Dr. Angela Sasse
(University College London)

Dr. Maximilian Schenk
(VZ Netzwerke)

Prof. Dr. Schwenk
(Ruhr Universität Bochum)

Joachim Seidelmann
(FhG IPA)

Prof. Dr. Jean-Pierre Seifert
(DTAG Labs)

Karl-Michael Sigl
(Bundeskriminalamt)

Prof. Dr. Indra Spiecker gen. Döhmann
(Karlsruhe Institute of Technology),

Prof. Dr. Sarah Spiekermann
(Wirtschaftsuniversität Wien)

Malte Spitz
(Bündnis 90 / Die Grünen)

Roland Stein
(IABG)

Prof. Dr. Heinz Thielmann
(Emphasys)

Dr. Sergey Tverdyshev
(Sysgo)

Dr. Alexander Walsch
(General Electric)

Dr. Georg Wambach
(T-Systems)

Axel Wiechel
(Vorwerk)

Oliver Winzenried
(Wibu-Systems)

Die im Bericht geäußerten Ansichten und Empfehlungen stehen ausschließlich in der Verantwortung der Promotoren und binden nicht die vorstehenden Firmen, Organisationen und Experten. Namensbeiträge sind als solche gekennzeichnet.

7 PROMOTORENGRUPPE SICHERHEIT

Autoren des Berichts:

Dr. Karsten Ottenberg (Vorsitz)
Vorsitzender
der Geschäftsführung,
Giesecke & Devrient

Susanne Kunschert
Mitglied
der Geschäftsführung, Pilz

Prof. Dr. Dr. h. c. mult.
August-Wilhelm Scheer
BITKOM

Die Autoren wurden unterstützt durch:

Fabian Bahr,
Giesecke & Devrient

Michael Barth,
BITKOM

Hansjörg Sperling-Wohlgemuth,
Pilz

Dr. Anne-Sophie Tombeil,
Fraunhofer IAO