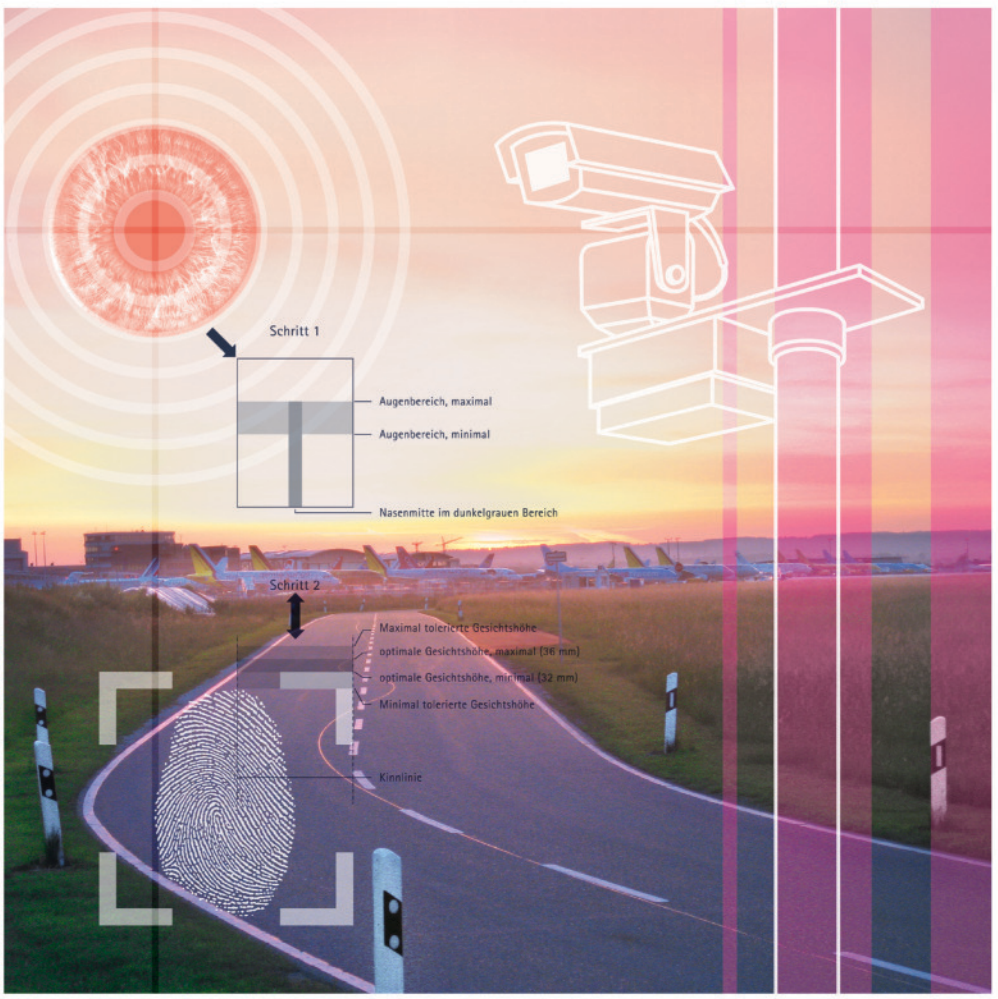
FAZIT Forschung
Schriftenreihe
Informations- und Medientechnologien in Baden-Württemberg

Bernd Hartmann, Andrea Buchholz,
Bernd Beckert (Hrsg.)

Sicherheit durch IT
Marktchancen und Herausforderungen am Beispiel Baden-Württemberg



Bernd Hartmann, Andrea Buchholz, Bernd Beckert (Hrsg.)

Sicherheit durch IT

Marktchancen und Herausforderungen am Beispiel Baden-Württemberg

Impressum

Herausgeber der FAZIT-Schriftenreihe:

MFG Stiftung Baden-Württemberg
Breitscheidstr. 4, D-70174 Stuttgart
Tel. +49 (0)711/90715-300, Fax +49 (0)711/90715-350

Zentrum für Europäische Wirtschaftsforschung GmbH (ZEW)
L 7,1, D-68161 Mannheim
Tel. +49 (0)621/1235-01, Fax +49 (0)621/1235-224

Fraunhofer-Institut für System- und Innovationsforschung (Fraunhofer ISI)
Breslauer Straße 48, D-76139 Karlsruhe
Tel. +49 (0)721/6809-0, Fax +49 (0)721/689152

Schutzgebühr € 8,-

ISSN 1861-5066

Inhaltsverzeichnis

1. EINFÜHRUNG 5

SICHERHEITSFORSCHUNG UND IHRE MARKTPOTENZIALE AM BEISPIEL BADEN-WÜRTTEMBERG 7
BEITRÄGE IN DIESEM BAND 8

2. IDENTITÄTSMANAGEMENT-SYSTEME IN BADEN-WÜRTTEMBERGISCHEN FIRMEN 10

METHODIK 10
EINSATZ VON IMS IN BADEN-WÜRTTEMBERG 11
GRÜNDE GEGEN DEN EINSATZ VOM IMS 15
FOLGEN DES EINSATZES VON IMS 17
ZUSAMMENFASSUNG UND AUSBLICK 22

3. GEBÄUDESICHERHEIT DURCH IT – FALLSTUDIE ANHAND DES FLUGHAFENS STUTTGART 23

DER FLUGHAFEN STUTTGART – RAHMENDATEN 24
METHODIK 25
SICHERHEIT UND SICHERHEITSKONZEPTE 25
DIE LEITSTELLE DES FLUGHAFENS 28
ANFORDERUNGEN AN SICHERHEITSSYSTEME 30
INNOVATIONSZYKLEN DER SICHERHEITSTECHNOLOGIE IN DER LEITSTELLE 32
GEBÄUDESICHERHEIT ALS CHANCE FÜR KMU 34
ZUSAMMENFASSUNG UND AUSBLICK 35

4. SICHERHEIT DURCH IT – FÜNF ANWENDUNGSSZENARIEN FÜR DAS JAHR 2020 37

WELCHE SICHERHEIT IST GEMEINT? 37
METHODE UND VORGEHEN 40
DIE FÜNF ANWENDUNGSSZENARIEN 45
ZUSAMMENFASSUNG UND AUSBLICK 64

5. AUSBLICK 65

6. LITERATUR 68

7. AUTOREN-, PROJEKT- UND PARTNERINFORMATION 72

Tabellenverzeichnis

Tabelle 1: Rangfolge der Flughäfen in Deutschland nach Passagierzahlen 2007 23
Tabelle 2: Ebenen der Sicherheit am Flughafen Stuttgart 26
Tabelle 3: Überblick über die betrachteten informationstechnischen Lösungen zur Erhöhung von Sicherheit 39
Tabelle 4: Ergebnis des Kombinationsschritts (Matrix) 43
Tabelle 5: Kombinationsmöglichkeiten aus der Perspektive der Technologien 45

Abbildungsverzeichnis

Abbildung 1: Einsatz von Identitätsmanagementsystemen nach Branche, in Prozent 12
Abbildung 2: Einsatz von Identitätsmanagementsystemen nach Betriebsgröße, in Prozent 12
Abbildung 3: Einsatz von Identitätsmanagementsystemen nach Nutzergruppe, in Prozent 13
Abbildung 4: Einsatz von Identitätsmanagementsystemen nach Betriebsgröße (Angaben in Prozent) 14
Abbildung 5: Nutzergruppen von IMS nach Branche (nur bei Einsatz), in Prozent 15
Abbildung 6: Kein Einsatz von IMS aufgrund der Kosten, nach Branche, in Prozent 16
Abbildung 7: Kein Einsatz vom IMS aufgrund von Nutzenerwägungen, nach Branche, in Prozent 16
Abbildung 8: Kein Einsatz von IMS aufgrund mangelnden Know-hows, nach Branche, in Prozent 17
Abbildung 9: Strukturiertere Unternehmensprozesse durch IMS-Einsatz, nach Branche, in Prozent 18
Abbildung 10: Strukturiertere Unternehmensprozesse durch IMS, nach Firmengröße, in Prozent 18
Abbildung 11: Reduktion von Ausfallzeiten durch IMS-Einsatz, nach Branche, in Prozent 19
Abbildung 12: Erhöhung der Sicherheit durch IMS-Einsatz, nach Branche, in Prozent 20
Abbildung 13: Erhöhung der Sicherheit durch IMS-Einsatz, nach Firmengröße, in Prozent 20
Abbildung 14: Erfüllung gesetzlicher Anforderungen durch IMS-Einsatz, nach Branche, in Prozent 21
Abbildung 15: Erfüllung gesetzlicher Anforderungen durch IMS-Einsatz, nach Firmengröße, in Prozent 21
Abbildung 16: Der Flughafen Stuttgart aus der Vogelperspektive 24
Abbildung 17: Sicherheitsrelevante Einzelsysteme unter Kontrolle durch die Leitstelle 29
Abbildung 18: Vernetzung im Rahmen des Sicherheitskonzepts am Flughafen Stuttgart 30
Abbildung 19: Fünf Einflussbereiche für die Szenarien 2020: „Sicherheit durch IT“ 40
Abbildung 20: Identifikation von plausiblen Kombinationssträngen am Beispiel des Anwendungsbereichs „Sicherheit im öffentlichen Raum“ 44
Abbildung 21: Kombinationen im Szenario: Sicherheit im öffentlichen Raum 46
Abbildung 22: Kombinationen im Szenario: Sicherheit im Auto, im öffentlichen Verkehr und im Flugverkehr 50
Abbildung 23: Kombinationen im Szenario: Sicherer Zugang zu Unternehmen und zum Smart Secure Home 55
Abbildung 24: Kombinationen im Szenario: Sicheres Online-Banking und Einkaufen im Internet 58
Abbildung 25: Kombinationen im Szenario: Medizin und Gesundheit 61

1. Einführung

Das Thema „Sicherheit“ ist zu einem zentralen Handlungsfeld des neuen Jahrtausends geworden – mit Herausforderungen für Wirtschaft, Wissenschaft und Politik gleichermaßen. Nicht nur die Bedrohung des eigenen Lebens durch Naturkatastrophen, Terrorismus oder Seuchen ist vermehrt in das Bewusstsein des Bürgers getreten, auch die Gefährdung, die durch Datenverlust oder den Verlust der eigenen digitalen Identität drohen, ist mit zunehmender Digitalisierung aller Bereiche von Wirtschaft und Gesellschaft zunehmend ein Thema geworden.

Besonders in der Informationstechnologie werden beide Dimensionen der Sicherheit deutlich: Informationstechnologie (IT) bietet das paradoxe Potenzial, das Leben sowohl sicherer als auch unsicherer zu machen. Einerseits bietet die zunehmende Vernetzung und die immer komplexer werdenden IT-Systeme ein immenses Bedrohungspotential, sowohl für die Privatnutzer an heimischen PCs oder WLAN-Hotspots, insbesondere aber auch für Unternehmen aller Größenlagen, Forschungseinrichtungen und öffentliche Organisationen. Es gibt niemand, der nicht durch Viren, Trojaner, Würmer und feindliche Angriffe bedroht wäre. Unter dem Begriff „IT-Sicherheit“ fallen alle entsprechenden Schutzmaßnahmen, um Hard- und Software sowie Netzwerke vor elektronischen und physischen Schäden zu bewahren. Dadurch, dass die gesamte Gesellschaft und insbesondere die Wirtschaft in eine immer größer werdende Abhängigkeit von IT gerät, muss IT-Sicherheit gewährleistet sein – sowohl innerhalb von Organisationen als auch in den Außenkontakten mit Geschäftspartnern. Dieses als „Sicherheit für IT“ zu umschreibende Feld ist ein großer Industriezweig mit zahlreichen Dienstleitungen geworden (vgl. Eckert 2004). Das Thema IT-Sicherheit im Sinne von „Sicherheit für IT“ wurde bereits in FAZIT untersucht (vgl. Bertschek/Döbler 2005). Neben dieser Perspektive, die auf die Sicherheitsbedrohungen durch Informationstechnologie hinweist, existiert jedoch noch eine komplementäre Perspektive, die auf „Sicherheit durch IT“ abhebt, also die Fähigkeit von Informationstechnologie, Sicherheit vor Bedrohungen zu schaffen. Dies umfasst die Systeme, Werkzeuge und Prozesse, mit Hilfe derer Staat, Bürger und Unternehmen geschützt werden können. Seit den Anschlägen vom 11. September 2001 wird darunter vor allem öffentliche Sicherheit verstanden (vgl. Niesing 2007, S. 8). Damit bewegt sich das Thema „Sicherheit durch IT“ im Spannungsfeld zwischen Kontrolle und Freiheit.

Mit dem Thema „Sicherheit durch IT“ sind spezielle Anwendungstechnologien im Bereich der Biometrie oder der Videoüberwachung eng verknüpft, die in der öffentlichen Debatte zu Reizthemen stilisiert wurden und deren Diskussion schnell in ideologische Grabenkämpfe abgleiten kann. Der Umgang mit diesen Themen erfordert jedoch ein kontinuierliches Analysieren der Chancen und Risiken, die mit den jeweiligen Technologien verbunden sind, damit Staat, Unternehmen und Bürger gleichermaßen eine ausgewogene und begründete Entscheidung für ein Sicherheitssystem treffen, das tatsächlich ein ausreichendes und krisensicheres Ausmaß an Sicherheit gewährleistet, ohne jedoch in Kontrolle und Überwachung abzugleiten.

Die leitenden Konzepte beim Thema „Sicherheit durch IT“ sind „Identifikation“ und „Authentifizierung. Authentifizierung dient der Feststellung, ob jemand wirklich derjenige ist, der er behauptet zu sein. Traditionellerweise geschieht dies über Mechanismen wie einen Schlüssel, PIN oder ein Passwort. Gleichzeitig sind dies Verfahren mit erheblichen Restrisiken – ein Passwort kann vergessen, ein Schlüssel geklaut, eine PIN verloren oder gestohlen worden sein. Identifikation hingegen geht noch einen Schritt weiter und hat das Ziel, herauszufinden, wer jemand überhaupt ist (vgl. Pfitzmann 2006).

Biometrische Verfahren der Authentifizierung oder Identifikation versprechen ein erheblich niedrigeres Restrisiko. Als Biometrie wird das Messen von Körper- oder Verhaltensmerkmalen bezeichnet. Gemessen werden können dabei etwa Körpermerkmale wie der Fingerabdruck, das Muster der Iris oder die Gesichtsform. Elektronisch lesbare biometrische Daten wie beispielsweise der Irisscan oder der so genannte elektronische Fingerabdruck können Personen zweifelsfrei identifizieren und weisen Zugangs- und Nutzungsrechte aus. Diese Form der Authentifizierung hat gegenüber den traditionellen Identifikationsmechanismen (z.B. Schlüssel, PIN, Passwort) den Vorteil, dass sie unverwechselbar mit einem Nutzer verbunden ist und entsprechend nicht verloren oder gestohlen werden kann. Damit wird nicht nur die Benutzerfreundlichkeit sondern auch die Sicherheit von Identifikationssystemen erheblich gesteigert. Gerade an Orten mit verschiedenen Sicherheitsstufen wie etwa Flughäfen erleichtern biometrische Verfahren die Implementierung von Sicherheitskonzepten deutlich. Herausforderungen für biometrische Systeme treten auf, je größer die Menge ist, aus der Menschen authentifiziert oder identifiziert werden sollen. Besonders im Fall der Identifizierung nimmt die Genauigkeit biometrischer Verfahren mit der Anzahl möglicher Personen stark ab (Pfitzmann 2006).

Während biometrische Daten der Identifizierung und Authentifizierung von Personen im Rahmen von Sicherheitskonzepten dienen, stehen auch zur Sicherung von Objekten und Flächen intelligente Sicherheitssysteme zur Verfügung. Insbesondere durch Bildverarbeitungstechnologien (Videosensorik) sollen automatisiert Umgebungen erfasst und komplexe Situationen interpretiert werden, etwa zum Objektschutz, zur Gebäude- oder Kraftfahrzeugsicherheit (vgl. Grasemann 2000, 2007a). Treiber dieser Entwicklung ist die Fähigkeit der Systeme, die Bilddaten auch zu interpretieren und Informationen von einer großen Anzahl von Sensoren sinnvoll zusammenzufügen (Pease 2006, S. 83). Kameras können so selbständig herrenlose Gepäckstücke in Flughäfen entdecken oder Autos, die in Tunnel in die falsche Richtung fahren. Technologischer Fortschritt zeigt sich hier insbesondere bei der Minimierung von Fehlalarmen – heute wird eine Erkennungsrate von über 95 Prozent erreicht (Pease 2006). Gerade bei sensiblen Überwachungsdaten wie sie beim Einsatz von Kameras in öffentlichen Räumen und Gebäuden vorkommen, kommt der automatisierten Bildverarbeitung eine entscheidende Rolle zu. Sie filtert potenzielle Gefährdungspotenziale heraus und leitet nur diese dem menschlichen Betrachter weiter. Dem Argument eines „Überwachungsstaates“, das die Diskussion über Kameras im öffentlichen Raum provoziert, lässt sich so entgegenhalten, dass die Masse an Aufzeichnungen niemals einem Menschen zur Ansicht kommen. Gleichzeitig erleichtert die automatische Bildverarbeitung auch die Arbeit der Mitarbeiter in Leitstellen, indem sie das Datenmaterial bereits vorselektiert und überkomplexe Aufzeichnungen auf ein bearbeitbares Maß

reduziert.

Aufgrund dieses deutlichen Nutzens reichen die Einsatzgebiete maschineller Bildverarbeitung schon heute von industriellen Anwendungen über die Medizintechnik bis zur Automobilbranche und Sicherheitstechnik. Das Marktvolumen beträgt derzeit schätzungsweise etwa 6,5 Mrd. Euro weltweit. Der Markt ist jedoch bei weitem noch nicht ausgereizt: die Wachstumsraten pro Jahr sind nach Expertenschätzungen nach wie vor im zweistelligen Bereich (Trage 2006b).

Mit dieser zunehmenden Relevanz des Themas „Sicherheit durch IT“ bieten sich aber auch neue Potenziale gerade für Unternehmen und Forschungseinrichtungen, die bereits heute einen Schritt voraus sind und die Geschäftschancen erkennen. Es ist daher nicht verwunderlich, dass Sicherheitsforschung eine wesentliche Rolle auch im 7. Forschungsrahmenprogramm der EU spielt.[1] Das Thema Sicherheit wird als eins der zehn Leitthemen im Unterbereich Kooperationen identifiziert und von 2007 bis 2013 werden hier insgesamt 1,4 Milliarden Euro Forschungsfördergelder investiert. IT-basierte Sicherheitstechnologien sind hierfür zentral. Sicherheit wird erkannt als Grundvoraussetzung für „Wohlstand, wirtschaftliche und gesellschaftliche Investitionen sowie Freiheit“. Sicherheit meint dabei: Sicherheit der Bürger, Sicherheit von Infrastrukturen und Versorgung, intelligente Überwachung und Grenzsicherheit, die Wiederherstellung von Sicherheit im Krisenfall sowie Querschnittsaktivitäten wie die Integration, Zusammenschaltung und Interoperabilität von Sicherheitssystemen, das Thema Sicherheit und Gesellschaft sowie schließlich die Koordinierung und Strukturierung der Sicherheitsforschung.

„Sicherheit durch IT“ ist branchenübergreifend von Bedeutung. In allen Bereichen der Wirtschaft werden sensible Daten übermittelt und verwendet und legen so die Nutzung von Identitätsmanagementsystemen nahe. Produktions- und Herstellungsprozesse im Maschinenbau erfordern reibungslos funktionierende Sicherheitssysteme etwa durch Videosensorik. Gleichzeitig besteht ein hohes Erfordernis an Sicherheitssystemen im öffentlichen Raum, etwa für die Abwendung von Katastrophen und terroristischen Anschlägen, d.h. auch öffentliche Auftraggeber haben einen steigenden Bedarf an IT-basierten Sicherheitssystemen.

Sicherheitsforschung und ihre Marktpotenziale am Beispiel Baden-Württemberg

Gerade für Unternehmen aus Baden-Württemberg existiert hier ein wachsender Markt. Durch starke Branchen wie Maschinenbau, Automotive, das Banken- und Versicherungswesen, aber auch öffentliche Institutionen vom Flughafen bis zum Fußballstadion besteht hier ein großer Nachfragermarkt, der idealerweise durch heimische Zulieferer bedient wird. Die starke Bedeutung, die Sicherheitsthemen in Baden-Württemberg bereits zugemessen wird, verdeutlicht sich auch in dem im Oktober 2007 gestarteten Innovationscluster „Future Security Baden Württem-

[1] Vgl. http://cordis.europa.eu/fp7/

berg“ unter Leitung der Fraunhofer-Gesellschaft.[2] Dieser Verbund aus Unternehmen, Universitäten, Forschungseinrichtungen und dem Innenministerium von Baden-Württemberg widmet sich der zivilen Sicherheitsforschung und der Entwicklung von innovativen Produkten und Dienstleistungen in der Sicherheitstechnologie gemeinsam mit den zukünftigen Anwendern. Das Innovationscluster unterteilt sich in vier Schwerpunktthemen: Kritische Verkehrsinfrastrukturen, Detektion und Identifikation von Explosivstoffen, Systemintegration sowie Security & Society. Sicherheitsforschung ist ein Bereich, der sehr unterschiedliche technologische Disziplinen zusammenführt: von der Sensorik über Mikrosystemtechnik und Life Sciences bis hin zur Informationstechnologie. Entsprechende Kompetenzen gibt es nicht nur in den Universitäten in Stuttgart, Karlsruhe, Freiburg und Konstanz und den Fraunhofer- und Max-Planck-Instituten, sondern auch in zahlreichen Unternehmen, vom KMU bis zum Konzern. Beteiligt am Innovationscluster sind so etwa neben EADS oder Siemens Gebäudetechnik auch die Karlsruher Firma Vitracom AG oder die Stuttgarter VISENSO GmbH – beide Experten für Bildverarbeitung und Visualisierung.

Beiträge in diesem Band

Dieser Band der FAZIT Forschungsreihe „Sicherheit durch IT“ widmet sich dem Entwicklungsstand von intelligenten Sicherheitssystemen und Identitätsmanagement und prüft Anwendungspotenziale für kleine und mittlere Unternehmen (KMU) in Baden-Württemberg. Dabei wurden empirische und konzeptionelle Forschungsansätze kombiniert.

Ziel von FAZIT ist es, den Status Quo eines Themas wie „Sicherheit durch IT“ in Baden-Württemberg durch empirische Untersuchungen zu erheben sowie die zukünftige Entwicklung zu prognostizieren. Aus dem Stand heute und der Situation im Jahr 2020 lassen sich Potenziale für Forschung und Entwicklung wie auch für neue Produkte und Dienstleistungen ableiten, die letztlich die baden-württembergische Wirtschaft stärken.

Im Rahmen der halbjährlichen FAZIT-Unternehmensbefragung wurde 2007 ein Fragenkomplex zum Thema Identitätsmanagement in baden-württembergischen Firmen abgefragt. Es wurde nach Einsatz, Hemmnissen bzw. Nutzen von Identitätsmanagementsystemen gefragt; die Ergebnisse sind nach Firmengröße und Branche unterteilt. Eine Auswertung dieser Ergebnisse findet sich in Kapitel 2 dieses Forschungsbands.

Ein weiterer Zugang zum Status Quo von Sicherheit durch IT in Baden-Württemberg stellt eine Fallstudie zum Thema Gebäudesicherheit in öffentlichen Räumen anhand des Flughafens Stuttgart dar (Kapitel 3). Durch eine teilnehmende Beobachtung in der Leitstelle des Flughafens sowie Einzelinterviews im Vor- und Nachgang wurden die IT-basierten Lösungen für verschiedene Bedrohungssituationen identifiziert, die Innovationsschübe im Zeitverlauf deutlich gemacht sowie idealtypische Chancen für KMU im Bereich Sicherheitstechnologie herausgearbeitet.

[2] Vgl. www.emi.fraunhofer.de/EMI-Links/InnovationsclusterFutureSecurityBW/

Die zukünftigen Entwicklungstrends werden schließlich durch eine Szenarioanalyse von Sicherheit durch IT im Jahr 2020 aufgezeigt (Kapitel 4). Es wurden fünf Szenarien zum Einsatz von IT-basierten Sicherheitssystemen im Jahr 2020 entwickelt. Heutige Bedrohungssituationen wurden dazu in die Zukunft projiziert und Technologien, die heute noch in der Entwicklung sind, als funktionsfähig und einsetzbar gedacht, um ihre Anwendungsfelder und Auswirkungen in der Zukunft zu beschreiben. Der Fokus liegt dabei auf Zugangs- und Identifikationstechnologien, die von der digitalen Videoüberwachung bis zu Biochips und Biosensoren reichen.

2. Identitätsmanagement-Systeme in baden-württembergischen Firmen[3]

Ein zentraler Aspekt von Sicherheit durch IT ist der Einsatz von Identitätsmanagement-Systemen (IMS). In allen Bereichen der Wirtschaft werden sensible Daten übermittelt und verwendet. So setzten fast 63 Prozent der baden-württembergischen Unternehmen computergestützte Systeme zur Unterstützung ihrer Geschäftsprozesse ein (vgl. Bertschek et. al. 2006). Informations- und Kommunikationstechnologien (IKT) werden im Geschäftsalltag immer mehr zu einer grundlegenden Voraussetzung aller Aktivitäten. Damit wächst die Notwendigkeit und der Bedarf an gleichermaßen technisch und rechtlich zuverlässiger wie auch akzeptierter Authentifizierung und Identifikation. Allerdings wird der individuelle Umgang mit diesen verschiedenen Identitäten umso komplizierter, je mehr IKT in alle Lebensbereiche des Einzelnen vordringen. Identitäten von Nutzern werden in IT-Systemen durch Datensätze repräsentiert. Mit Hilfe von IMS lassen sich diese Datensätze verwalten: Zum einen können IMS steuern, wer in welchem Kontext Nutzerdaten erhält und wie diese verwendet werden dürfen. Zum anderen können IMS mindestens dokumentieren, wer welche Nutzerdaten erhält und wie er diese verwenden sollte. Ziel von IMS ist stets die Vereinfachung der Internetkommunikation für den Einzelnen, ohne dass hiermit eine Verringerung der Sicherheit und des Datenschutzes einhergeht. Einfache IMS übernehmen für den Nutzer die Passwort- und Zugangsverwaltung, komplexere Systeme regeln ein umfassendes situationsbezogenes Pseudonymmanagement. Sowohl für die IKT-Anwender, als auch für die IKT-Anbieter, deren Image wesentlich von einem seriösen Umgang mit sensiblen Daten abhängt, ist ein zuverlässiges IMS von Interesse.

Methodik

Im Rahmen der fünften FAZIT-Unternehmensbefragung wurden im Oktober und November 2007 ca. 9.000 baden-württembergische Unternehmen zu den Themen Unternehmenssoftware und eingebettete Systeme befragt (vgl. Bertschek et al. 2008). Die befragten Branchen unterteilen sich in den IT- und Mediensektor, Verkehrsdienstleister, das verarbeitende Gewerbe, das Bank- und Versicherungsgewerbe sowie technische Dienstleister. Ein Fragekomplex beschäftigte sich auch mit dem Status von IMS in baden-württembergischen Firmen. Es wurde nach Einsatz, Hemmnissen bzw. Nutzen von IMS gefragt. Die Ergebnisse sind nach Firmengröße und Branche unterteilt. Mit insgesamt 1.191 ausgefüllten Fragebogen, die zurückgesandt wurden, liegt die Responsequote bei 17 Prozent. Die Ergebnisse wurden soweit möglich auf die zugrunde liegende Grundgesamtheit hochgerechnet.

[3] Dieser Beitrag wurde erstellt unter Nutzung der Ergebnisse der Unternehmensbefragung baden-württembergischer Firmen im Herbst/Winter 2007 durch das Zentrum für Europäische Wirtschaft (ZEW), Mannheim.

Abgefragt wurde zunächst der Einsatz bzw. Nichteinsatz von IMS in allen Branchen. Wird ein IMS eingesetzt, wurde weiterhin gefragt, für welche Nutzergruppe es eingesetzt wird: Kunden, Mitarbeiter oder beide. Ferner wurde nach den Folgen der Einführung eines IMS im Unternehmen gefragt: Sind dadurch strukturiertere Unternehmensprozesse entstanden, haben sich Ausfallzeiten aufgrund von Zugriffsproblemen reduziert, hat sich die Sicherheit erhöht oder wurden dadurch gesetzliche Anforderungen erfüllt?

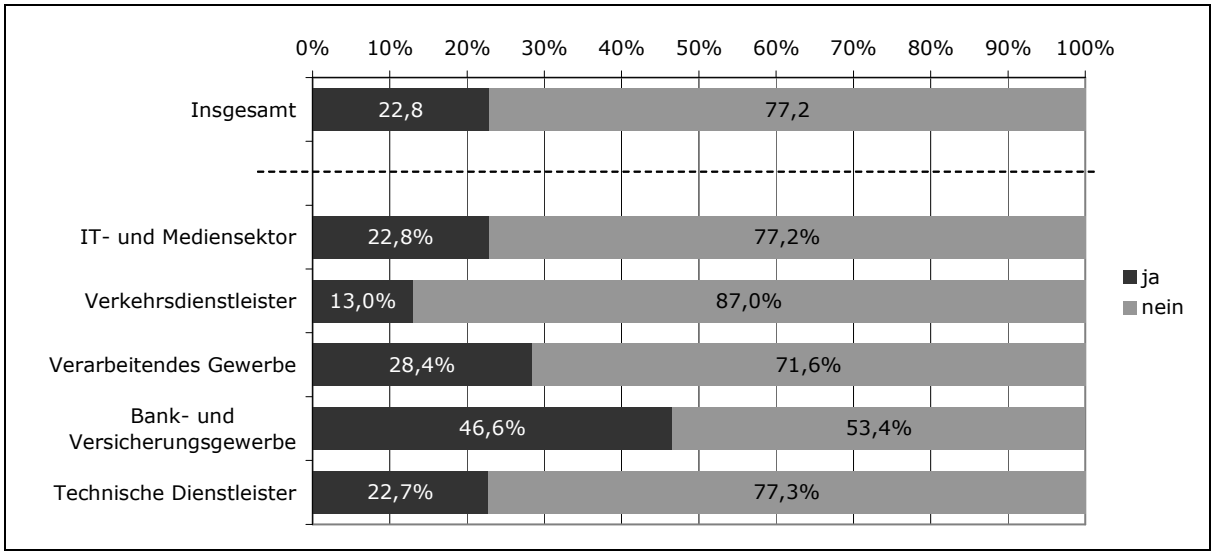
Sollte in dem Unternehmen noch kein IMS eingesetzt werden, wurde danach gefragt, ob es innerhalb der nächsten zwei Jahre geplant ist oder derzeit noch keine Planungen existieren. Schließlich wurden auch die Gründe erfragt, wegen derer kein IMS im Unternehmen eingesetzt wird: zu hohe Kosten, zu geringer bzw. nicht einschätzbarer Nutzen oder fehlendes Know-how im Unternehmen. Mehrfachnennungen waren möglich.

Einsatz von IMS in Baden-Württemberg

Insgesamt zeigt die Unternehmensbefragung, dass der Einsatz von IMS in Baden-Württemberg branchenübergreifend noch relativ gering ausgeprägt ist. Weniger als ein Viertel der befragten Unternehmen setzt IMS ein (22,8 Prozent), entsprechend kommt in mehr als drei Viertel der Unternehmen kein IMS zum Einsatz (77,2 Prozent).

Beim Blick auf die einzelnen Branchen (vgl. Abbildung 1) zeigen sich gewisse Varianzen: Mit 46,6 Prozent werden Identitätsmanagement-Systeme am häufigsten im Bank- und Versicherungsgewerbe eingesetzt, d.h. knapp die Hälfte aller Unternehmen in diesem Bereich setzt bereits IMS ein. Aufgrund der hochsensiblen Daten im Bank- und Versicherungsbereich ist die erhöhte Sensibilität für IT-Sicherheitssysteme in dieser Branche nicht überraschend. Die geringste Ausprägung zeigt der Einsatz von IMS bei den Verkehrsdienstleistern mit nur 13 Prozent. In den übrigen Branchen liegen die Einsatzwerte um 25 Prozent.

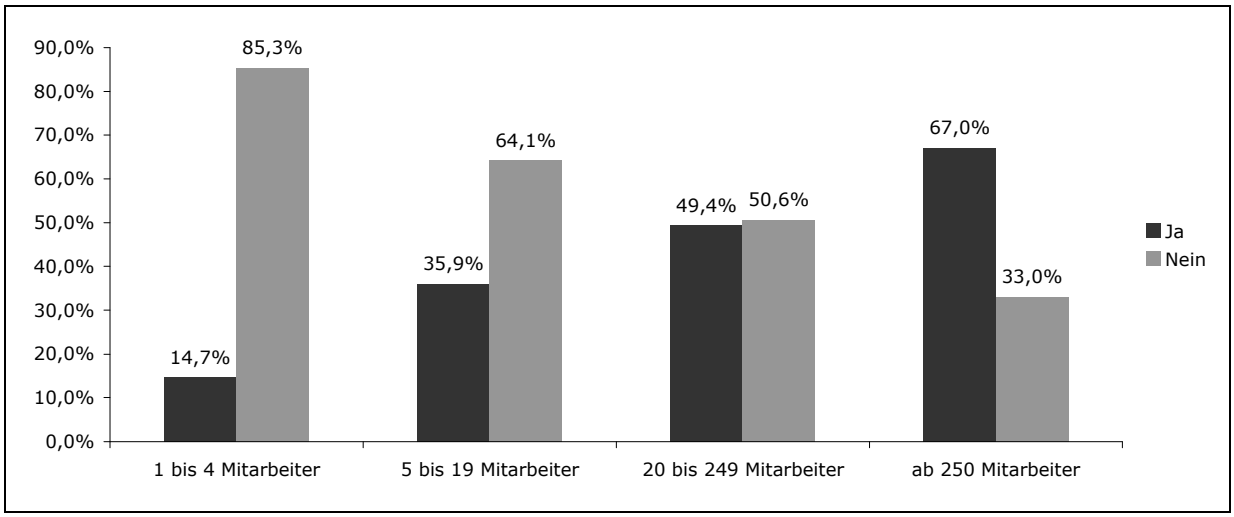
Abbildung 1: Einsatz von Identitätsmanagementsystemen nach Branche, in Prozent



Anmerkung: Angaben hochgerechnet auf die der Befragung zugrunde liegende Grundgesamtheit.
Quelle: FAZIT-Unternehmensbefragung, Herbst/Winter 2007; Berechnungen des ZEW.

Wenig überraschend ist hingegen die Erkenntnis, dass die Nutzung von IMS mit zunehmender Firmengröße ebenfalls zunimmt. Schwerpunkte der Nutzung liegen bei den klassischen KMU (zwischen 20 und 250 Mitarbeitern) mit knapp 50 Prozent sowie Unternehmen ab 250 Mitarbeitern, bei denen über zwei Drittel der nutzenden Unternehmen verortet sind (vgl. Abbildung 2).

Abbildung 2: Einsatz von Identitätsmanagementsystemen nach Betriebsgröße, in Prozent



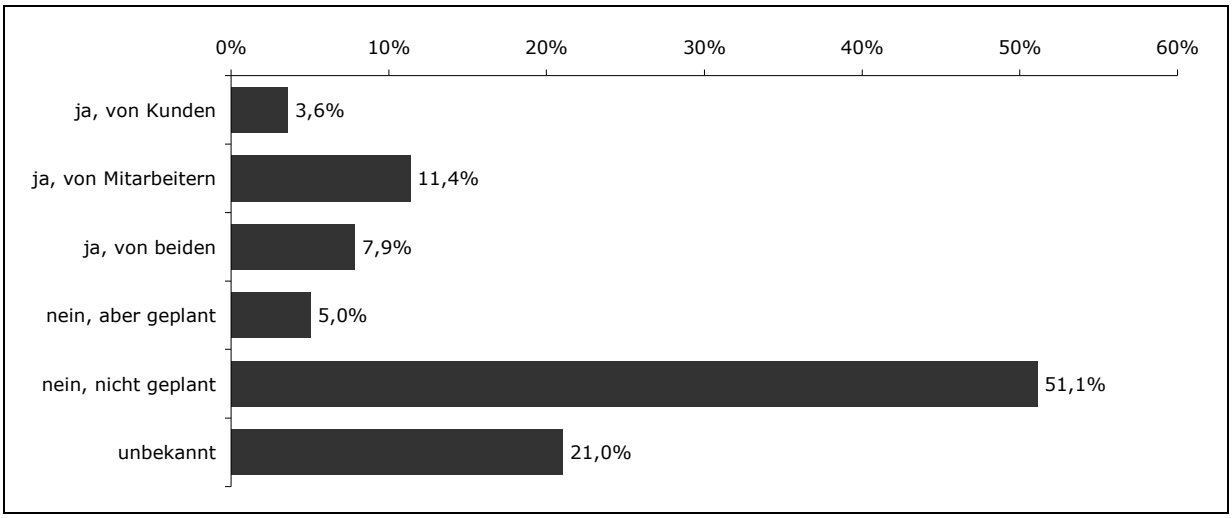
Anmerkung: Angaben hochgerechnet auf die der Befragung zugrunde liegende Grundgesamtheit.
Quelle: FAZIT-Unternehmensbefragung, Herbst/Winter 2007; Berechnungen des ZEW.

Von den befragten Unternehmen nutzen 11,4 Prozent ein IMS für das Management der Identitäten der eigenen Mitarbeiter (vgl. Abbildung 3). Dies ist damit der häufigste Nutzungszweck unter den Unternehmen, die ein IMS einsetzen. 7,9 Prozent der befragten Unternehmen hat ein IMS im Einsatz für das Management der Identitäten sowohl der eigenen Mitarbeiter wie auch der Kunden. Nur 3,6 Prozent aller Unternehmen nutzt ein IMS ausschließlich für das Management der Identitäten der Kunden.

Dem Einsatz nach Nutzergruppen steht die große Zahl der Unternehmen gegenüber, die kein IMS einsetzen: Rund die Hälfte aller befragten Unternehmen haben kein IMS im Einsatz und haben auch keinen Einsatz in der Zukunft geplant. Lediglich fünf Prozent der Unternehmen sehen in den nächsten zwei Jahren einen Einsatz vor.

Kritisch ist die Zahl der Unternehmen, denen der Begriff Identitätsmanagement-System unbekannt ist: Mit 21 Prozent herrscht bei mehr als einem Fünftel der befragten Unternehmen darüber Unkenntnis.

Abbildung 3: Einsatz von Identitätsmanagementsystemen nach Nutzergruppe, in Prozent

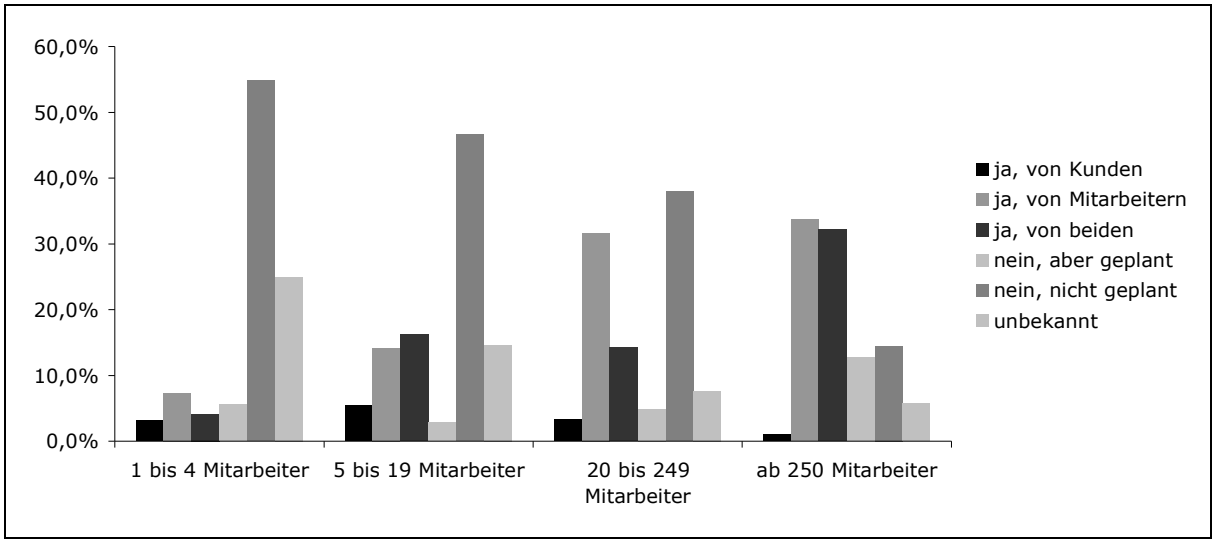


Anmerkung: Angaben hochgerechnet auf die der Befragung zugrunde liegende Grundgesamtheit.
Quelle: FAZIT-Unternehmensbefragung, Herbst/Winter 2007; Berechnungen des ZEW.

Bei einem erneuten Blick auf die Betriebsgröße wird auch hier deutlich, dass sich die Nutzungssituation deutlich zwischen kleinen und größeren Unternehmen unterscheidet. Insbesondere zeigt sich, wie durch IMS bei zunehmender Betriebsgröße von der reinen Nutzung für die eigenen Mitarbeiter die Systeme auch zunehmend für das Identitätsmanagement der Kunden eingesetzt werden. Bei Unternehmen mit über 250 Mitarbeitern hält sich die Nutzung von IMS für die eigenen Mitarbeiter (33,7 Prozent) mit der Nutzung für Kunden und Mitarbeiter gleichermaßen (32,3 Prozent) fast die Waage. In der Unternehmensgröße ab 250 Mitarbeitern herrscht auch nur eine geringe Unkenntnis von IMS (5,7 %), und der Anteil der Unternehmen, die planen, ein IMS einzusetzen (12,8 Prozent) ist fast gleichwertig mit der Zahl der Unternehmen, die dies nicht planen (14,5 Prozent). Zum Vergleich: Bei Unternehmen unter 20 Mitarbeitern hat rund die Hälfte der befragten Unternehmen keinen Einsatz von IMS auch in Zukunft geplant.

Es lässt sich also festhalten: IMS kommen in Baden-Württemberg derzeit vor allem in größeren Unternehmen ab 250 Mitarbeitern zum Einsatz. Hier werden IMS nicht nur für die Mitarbeiter, sondern häufig bereits auch für die Kunden eingesetzt. Bei Unternehmen dieser Größe ist zu erwarten, dass der Kundenstamm ebenfalls größer ist als bei kleinen Unternehmen, daher macht hier der Einsatz von IMS auch schneller Sinn.

Abbildung 4: Einsatz von Identitätsmanagementsystemen nach Betriebsgröße (Angaben in Prozent)



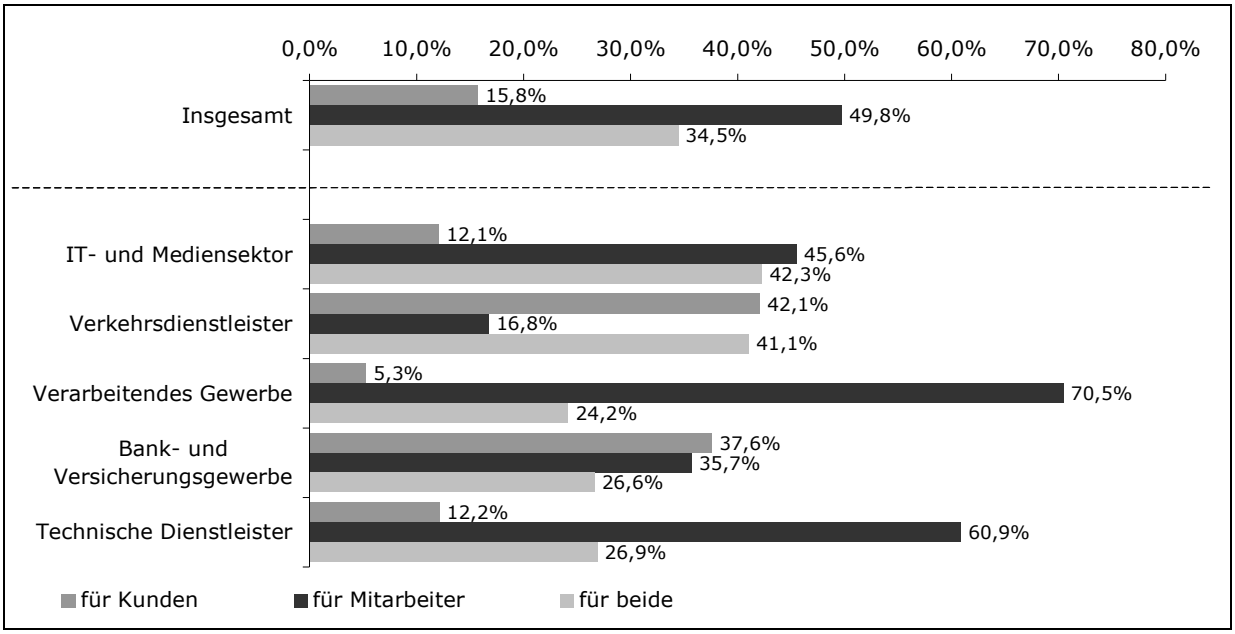
Anmerkung: Angaben hochgerechnet auf die der Befragung zugrunde liegende Grundgesamtheit
Quelle: FAZIT-Unternehmensbefragung, Herbst/Winter 2007; Berechnungen des ZEW.

Bei einer branchenbezogenen Sicht werden ebenfalls klare Unterschiede der Ausprägungen des Einsatzes von IMS für verschiedene Nutzergruppen deutlich (Abbildung 5). Insbesondere fällt der überdurchschnittliche Einsatz von IMS nur für die eigenen Mitarbeiter im verarbeitenden Gewerbe (70,5 Prozent) und bei den technischen Dienstleistern (60,9 Prozent) ins Auge.

Die größte Ausprägung von IMS nur für Kunden zeigt sich hingegen im Bank- und Versicherungsgewerbe mit 37,5 Prozent. Im IT- und Mediensektor hingegen sind die Nutzung von IMS für die eigenen Mitarbeiter (45,6 Prozent) wie für Kunden und Mitarbeiter zusammen (42,3 Prozent) in etwa gleichwertig.

Diese Zahlen machen vor allem die jeweiligen Branchenstrukturen und ihre digitalen Arbeitsprozesse deutlich: Stark serviceorientierte Branchen wie das Bank- und Versicherungsgewerbe oder der IT- und Mediensektor haben häufige Kundenkontakte, die auch das Management der Identitäten von Kunden erforderlich machen. Im verarbeitenden Gewerbe und bei den technischen Dienstleistern hingegen steht vor allem das Management der internen Arbeitsprozesse im Vordergrund.

Abbildung 5: Nutzergruppen von IMS nach Branche (nur bei Einsatz), in Prozent



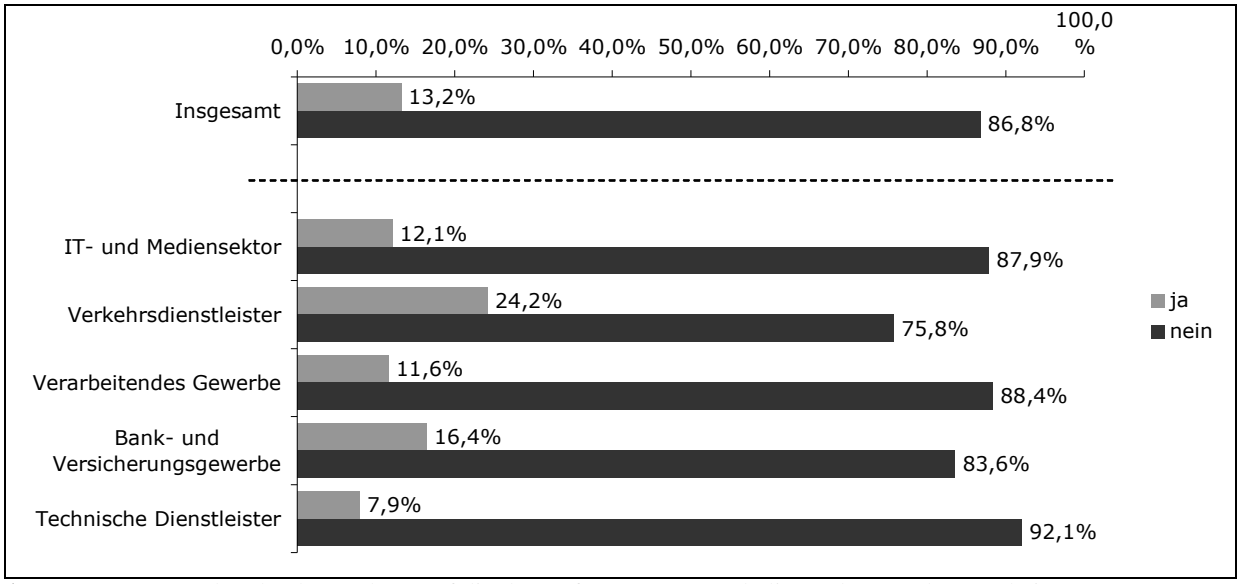
Anmerkung: Angaben hochgerechnet auf die der Befragung zugrunde liegende Grundgesamtheit.
Quelle: FAZIT-Unternehmensbefragung Herbst/Winter 2007; Berechnungen des ZEW

Gründe gegen den Einsatz vom IMS

Angesichts der großen Zahl an baden-württembergischen Unternehmen, die kein IMS einsetzen und dies auch nicht vorhaben, lohnt sich ein genauer Blick auf die Gründe, die aus Unternehmenssicht dagegen sprechen.

Unter den Unternehmen, die Sicherheitssysteme kennen, aber nicht planen, sie einzusetzen, geschieht dies nicht aus Kostenerwägungen. Nur 13,2 Prozent der Unternehmen haben dies als Grund genannt – die überwiegende Mehrheit von 86,8 Prozent sieht darin keinen Grund (vgl. Abbildung 6). Auch branchenspezifisch gibt es kaum Unterschiede – einzig bei den Verkehrsdienstleistern scheinen Kostengründe mit rund 25 Prozent eine stärkere Rolle zu spielen als bei den anderen Branchen.

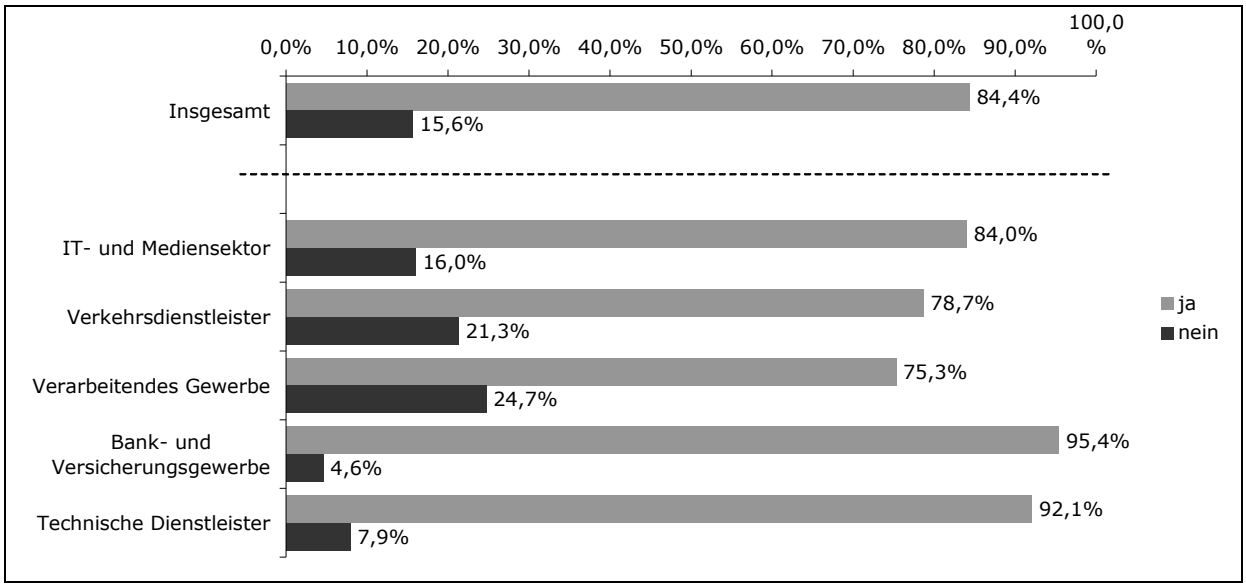
Abbildung 6: Kein Einsatz von IMS aufgrund der Kosten, nach Branche, in Prozent



Anmerkung: Angaben hochgerechnet auf die der Befragung zugrunde liegende Grundgesamtheit.
Quelle: FAZIT-Unternehmensbefragung Herbst/Winter 2007; Berechnungen des ZEW

Der überwiegende Grund für die Ablehnung von IMS scheint sehr deutlich in einem nicht wahrgenommenen Nutzen zu liegen. Rund 85 Prozent der befragten Unternehmen, die kein IMS einsetzen, führen Nutzenerwägungen als Grund für die Ablehnung an (vgl. Abbildung 7).

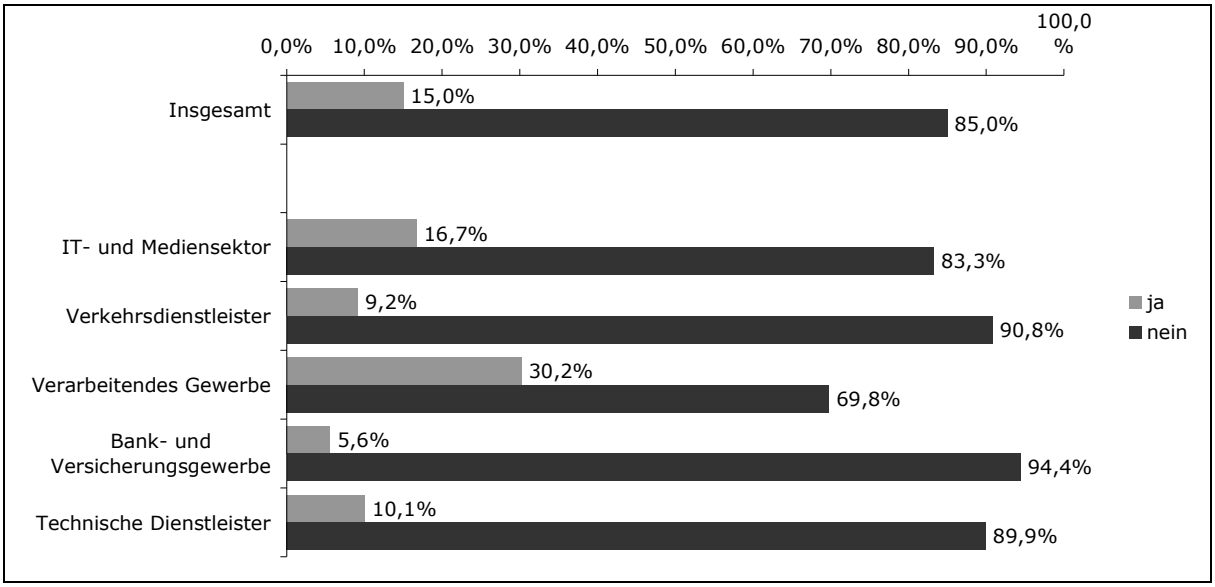
Abbildung 7: Kein Einsatz vom IMS aufgrund von Nutzenerwägungen, nach Branche, in Prozent



Anmerkung: Angaben hochgerechnet auf die der Befragung zugrunde liegende Grundgesamtheit
Quelle: FAZIT-Unternehmensbefragung Herbst/Winter 2007; Berechnungen des ZEW

Ein ähnlich unbedeutender Grund wie die Kosten scheint auch mangelndes Know-how zu sein: Nur 15 Prozent der befragten Unternehmen sehen darin eine Ursache (vgl. Abbildung 8). Im Bank- und Versicherungsgewerbe ist der Wert mit 5,6 Prozent sogar besonders niedrig ausgeprägt.

Abbildung 8: Kein Einsatz von IMS aufgrund mangelnden Know-hows, nach Branche, in Prozent



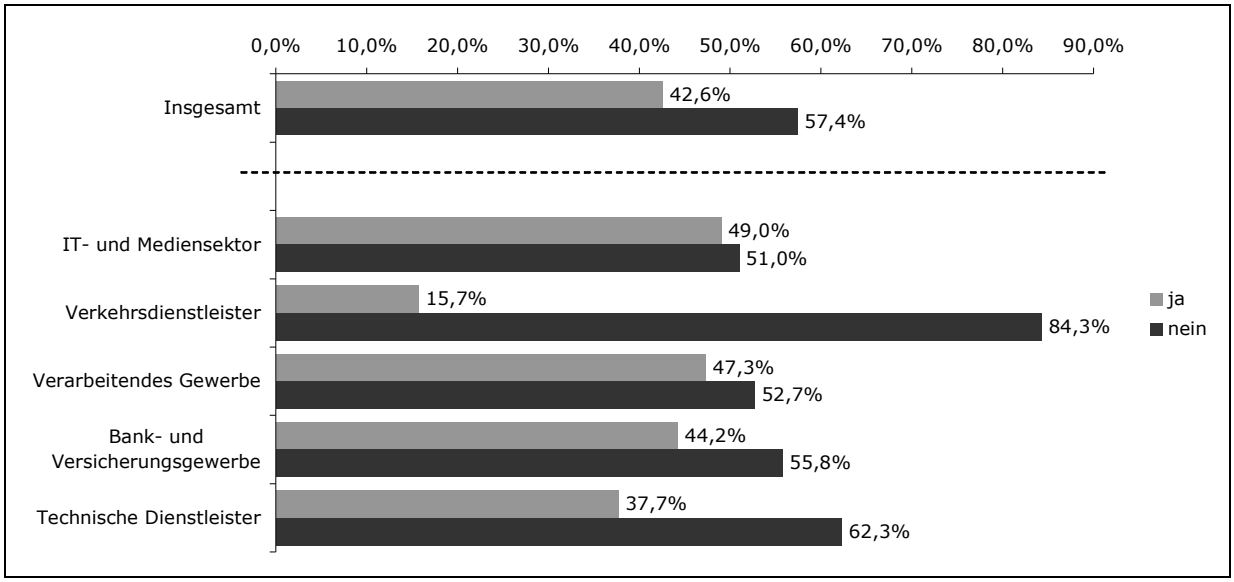
Anmerkung: Angaben hochgerechnet auf die der Befragung zugrunde liegende Grundgesamtheit
Quelle: FAZIT-Unternehmensbefragung Herbst/Winter 2007; Berechnungen des ZEW

Folgen des Einsatzes von IMS

Während also vor allem der mangelnde wahrgenommene Nutzen der Hauptgrund für den Verzicht auf den Einsatz eines IMS ist, sind dementsprechend die Folgen, die der Einsatz eines IMS für ein Unternehmen hat, sehr aufschlussreich. Worin sehen diese Unternehmen den Nutzen und die Folgen des Einsatzes von IMS in ihrem Unternehmen?

Eine solche mögliche Folge wären strukturiertere Unternehmensprozesse. Hat das IMS aus Sicht der Unternehmen deutlichen Einfluss auf die internen Prozesse? Die Antwort auf diese Frage fällt zwischen den einzelnen Branchen stark unterschiedlich aus. Insgesamt sehen etwas unter der Hälfte der befragten Unternehmen (42,6 Prozent) deutliche Auswirkungen auf die Unternehmensprozesse, während die knappe Mehrheit (57,4 Prozent) dies nicht so sieht (vgl. Abbildung 9). Auf einzelne Branchen bezogen fallen deutlich die Verkehrsdienstleister heraus, von denen mit 84,3 Prozent die überwiegende Mehrheit keine Veränderungen auf die Prozesse sieht. Auch bei den technischen Dienstleistern gibt mit 62,3 Prozent der befragten Unternehmen eine deutliche Mehrheit an, keine Auswirkungen auf die Prozesse zu sehen. Im IT- und Mediensektor hingegen halten sich die Ansichten in etwa die Waage. Es lässt sich annehmen, dass das Ergebnis stark von den in der jeweiligen Branche auch ansonsten üblichen Prozessorientierung abhängt, inwieweit die Einführung eines IMS hier einen deutlich spürbaren Unterschied macht.

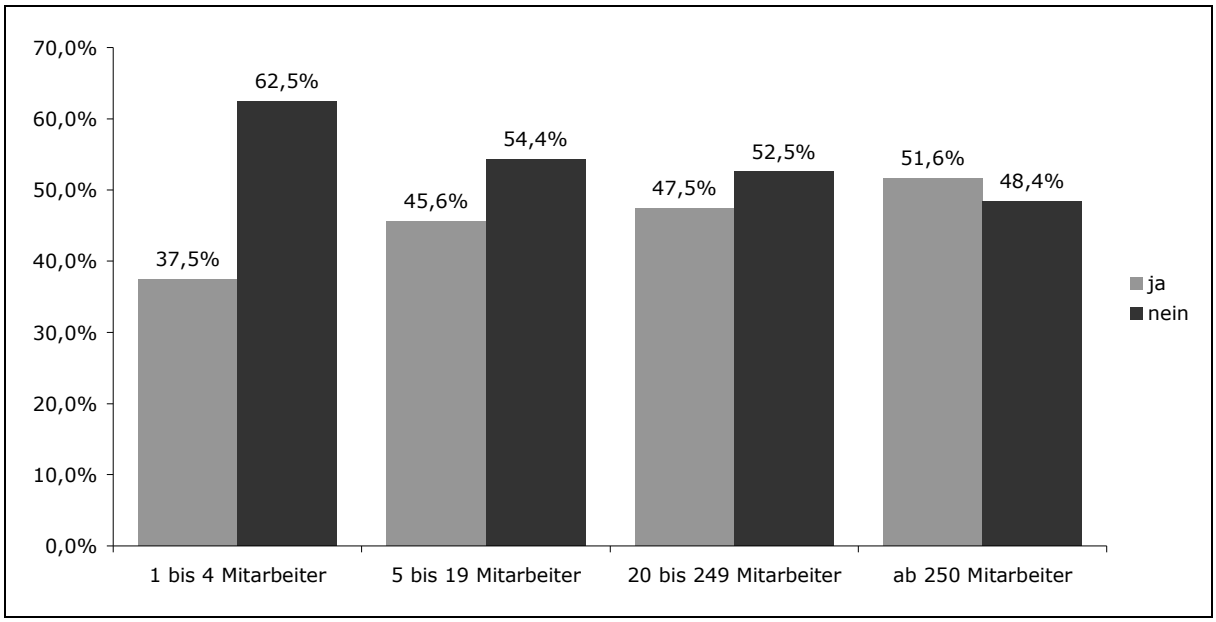
Abbildung 9: Strukturiertere Unternehmensprozesse durch IMS-Einsatz, nach Branche, in Prozent



Anmerkung: Angaben hochgerechnet auf die der Befragung zugrunde liegende Grundgesamtheit
Quelle: FAZIT-Unternehmensbefragung Herbst/Winter 2007; Berechnungen des ZEW

Ein Blick auf die Firmengröße offenbart auch hier: Je größer das Unternehmen, desto eher wird ein positiver Einfluss auf die Unternehmensprozesse erkannt (vgl. Abbildung 10).

Abbildung 10: Strukturiertere Unternehmensprozesse durch IMS, nach Firmengröße, in Prozent

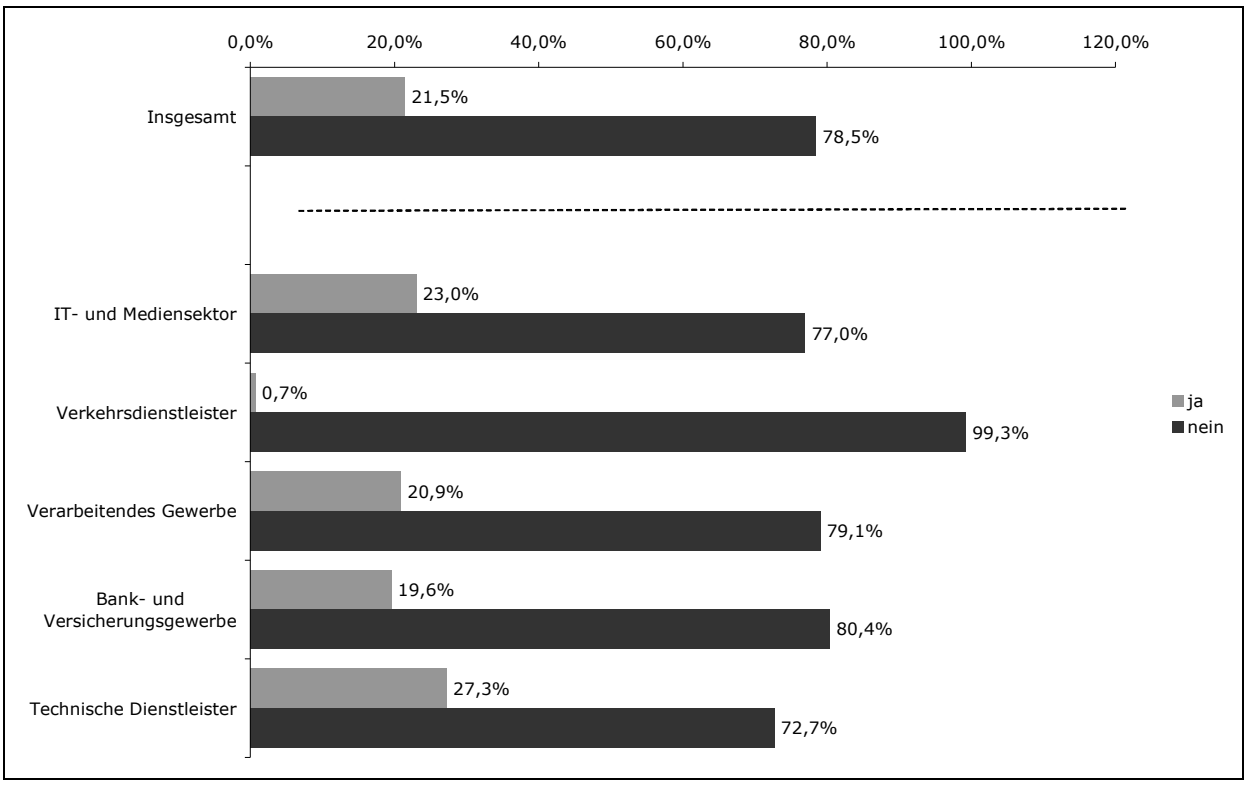


Anmerkung: Angaben hochgerechnet auf die der Befragung zugrunde liegende Grundgesamtheit
Quelle: FAZIT-Unternehmensbefragung Herbst/Winter 2007; Berechnungen des ZEW

Deutlicher sind die Ergebnisse im Hinblick auf die Ausfallzeiten: Nur rund ein Fünftel der befragten Unternehmen sieht durch den Einsatz eines IMS deutlich reduzierte Ausfallzeiten als Folge (vgl. Abbildung 11). Unter Ausfallzeiten fällt hier etwa die Verhinderung des Arbeitens aufgrund von Identifizierungsproblemen am Rechner. Besonders deutlich fällt abermals die Antwort der Verkehrsdienstleister aus, die mit 99,3 Prozent nahezu übereinstimmend keine

Reduktion von Ausfallzeiten durch IMS-Einsatz in ihrer Branche erkennen können.

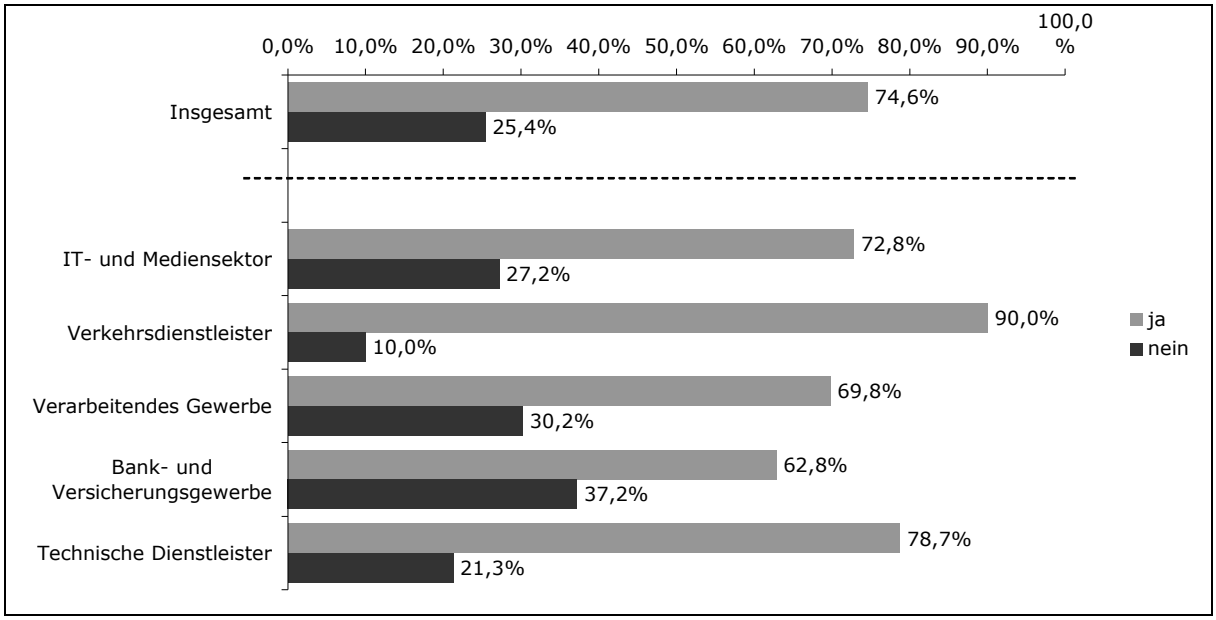
Abbildung 11: Reduktion von Ausfallzeiten durch IMS-Einsatz, nach Branche, in Prozent



Anmerkung: Angaben hochgerechnet auf die der Befragung zugrunde liegende Grundgesamtheit
Quelle: FAZIT-Unternehmensbefragung Herbst/Winter 2007; Berechnungen des ZEW

Die deutlichste Folge – und damit der Hauptgrund für den Einsatz von IMS – ist eine spürbar erhöhte Sicherheit. Rund drei Viertel aller Unternehmen, die IMS einsetzen, sieht dies als klare Folge. Abermals weisen die Verkehrsdienstleister einen besonders hohen Wert auf: 90 Prozent der befragten Unternehmen dieser Branche sehen die Erhöhung der Sicherheit als Folge. Im Bank- und Versicherungsgewerbe sind dies überraschend lediglich 62,8 Prozent.

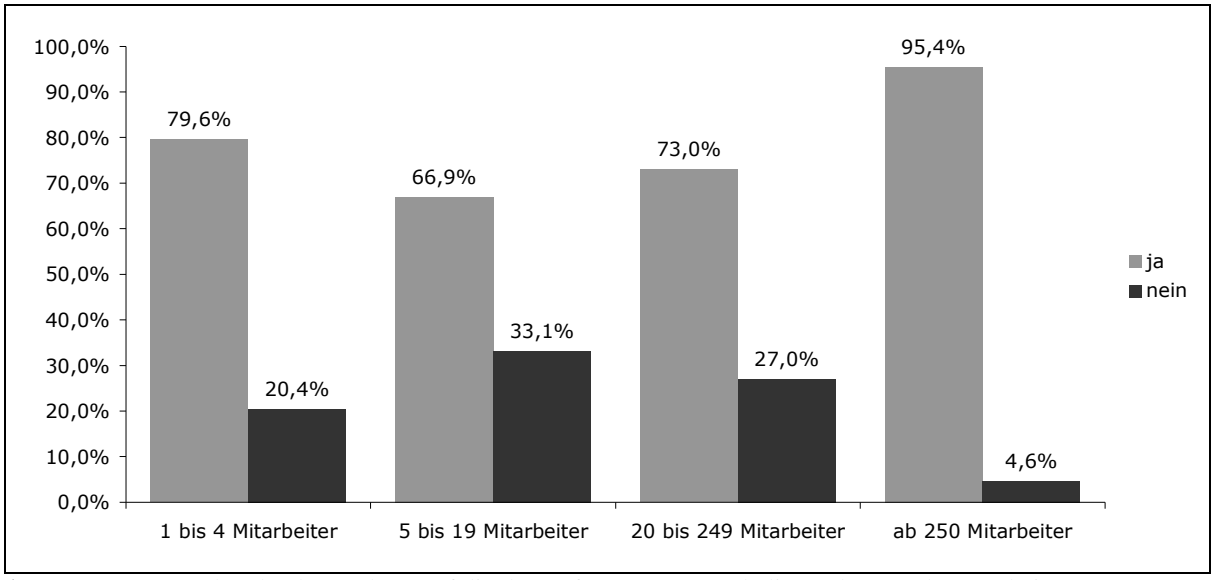
Abbildung 12: Erhöhung der Sicherheit durch IMS-Einsatz, nach Branche, in Prozent



Anmerkung: Angaben hochgerechnet auf die der Befragung zugrunde liegende Grundgesamtheit
Quelle: FAZIT-Unternehmensbefragung Herbst/Winter 2007; Berechnungen des ZEW

Die Zustimmung zu mehr Sicherheit als Folge von IMS ist auch über alle Firmengrößen hinweg deutlich vorhanden. Mit 95,4 Prozent Zustimmung liegt der Wert aber bei den großen Unternehmen über 250 Mitarbeitern ganz besonders hoch (vgl. Abbildung 13).

Abbildung 13: Erhöhung der Sicherheit durch IMS-Einsatz, nach Firmengröße, in Prozent

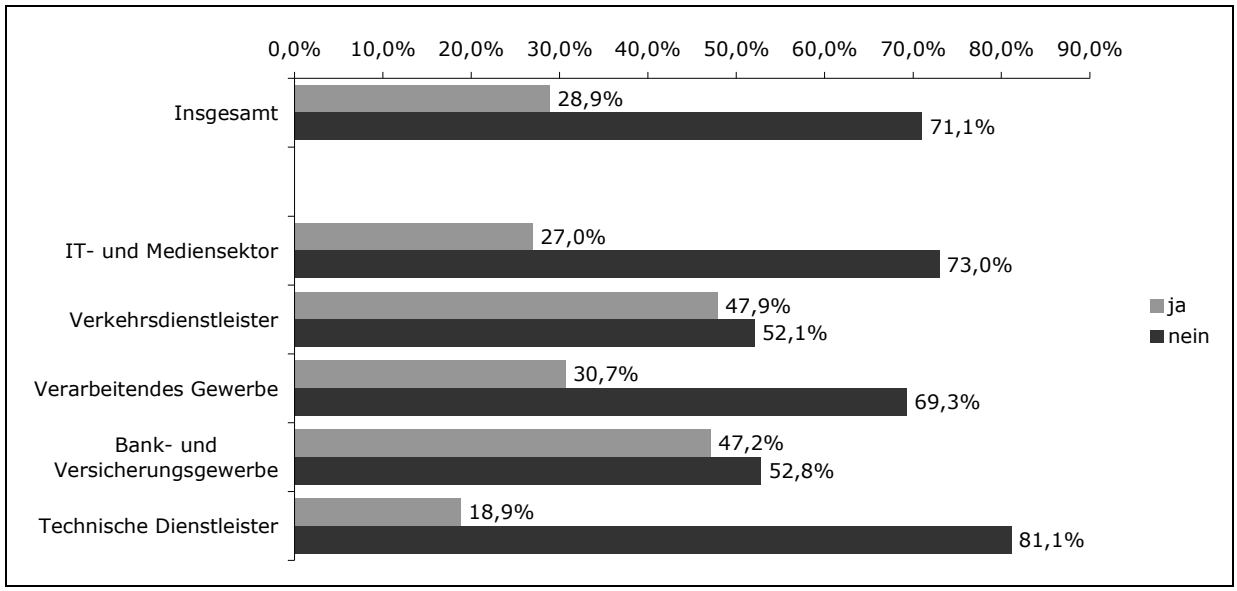


Anmerkung: Angaben hochgerechnet auf die der Befragung zugrunde liegende Grundgesamtheit
Quelle: FAZIT-Unternehmensbefragung Herbst/Winter 2007; Berechnungen des ZEW

Ein möglicher Grund und eine Folge des Einsatzes von IMS in Unternehmen kann auch die Erfüllung von gesetzlichen Anforderungen sein. Im Schnitt wird darin eine weniger relevante Folge gesehen – mit 71,1 Prozent stimmen über zwei Drittel der befragten Unternehmen dem nicht zu, bei den technischen Dienstleistern sind dies gar 81,1 Prozent. Lediglich im Bank- und

Versicherungsgewerbe sieht mit 47,2 Prozent der befragten Unternehmen knapp die Hälfte der Unternehmen hier eine Relevanz – angesichts der sensiblen Daten in dieser Branche ist dies naheliegend.

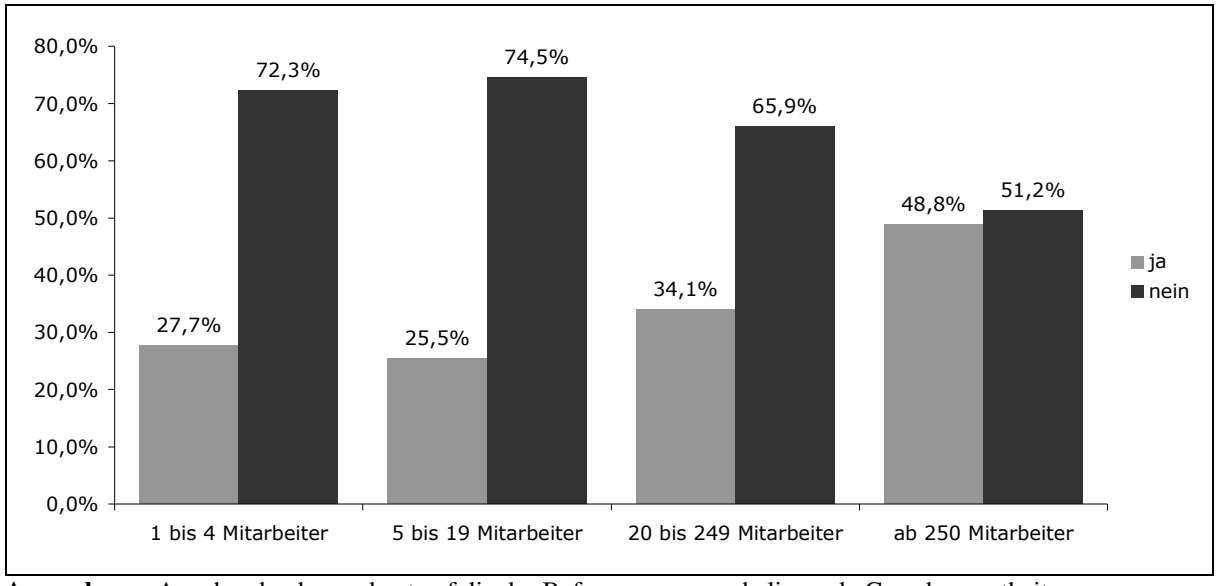
Abbildung 14: Erfüllung gesetzlicher Anforderungen durch IMS-Einsatz, nach Branche, in Prozent



Anmerkung: Angaben hochgerechnet auf die der Befragung zugrunde liegende Grundgesamtheit
Quelle: FAZIT-Unternehmensbefragung Herbst/Winter 2007; Berechnungen des ZEW

Die Erfüllung gesetzlicher Anforderungen wird ebenfalls erst bei Unternehmen ab 250 Mitarbeitern mit einer gewissen Relevanz eingestuft. In dieser Firmenkategorie stimmen 48,8 Prozent der befragten Unternehmen der Aussage zu, dass der Einsatz von IMS die Erfüllung gesetzlicher Anforderungen als Folge haben kann.

Abbildung 15: Erfüllung gesetzlicher Anforderungen durch IMS-Einsatz, nach Firmengröße, in Prozent



Anmerkung: Angaben hochgerechnet auf die der Befragung zugrunde liegende Grundgesamtheit
Quelle: FAZIT-Unternehmensbefragung Herbst/Winter 2007; Berechnungen des ZEW

Zusammenfassung und Ausblick

Die Auswertung der Umfrageergebnisse zu Identitätsmanagement in baden-württembergischen Firmen hat deutlich gemacht, dass die Themenrelevanz noch unterdurchschnittlich in der Unternehmenspraxis gelebt wird. Konkret bedeutet dies, dass branchenübergreifend weniger als die Hälfte der Unternehmen bereits IMS einsetzen. In einzelnen Branchen wie dem Bank- und Versicherungsgewerbe ist der Einsatz noch am stärksten ausgeprägt und reicht fast an die 50 Prozent heran. Bei Verkehrsdienstleistern hingegen liegt der Anteil bei nur knapp über zehn Prozent. Der IT- und Mediensektor weist eine Nutzung auf, die nahe dem branchenübergreifenden Durchschnitt ist.

Wenig überraschend ist hingegen die Erkenntnis, dass die Nutzung von Identitätsmanagementsystemen mit zunehmender Firmengröße ebenfalls zunimmt. Schwerpunkte der Nutzung liegen bei den klassischen KMU (zwischen 20 und 250 Mitarbeitern) mit knapp 50 Prozent sowie Unternehmen ab 250 Mitarbeitern, bei denen über zwei Drittel der nutzenden Unternehmen verortet sind. Am häufigsten werden Identitätsmanagementsysteme bei den eigenen Mitarbeitern eingesetzt, gefolgt vom Einsatz für Kunden und Mitarbeiter gleichermaßen. Der Einsatz nur für den Kunden ist sehr selten.

Bei den Unternehmen, die keine Identitätsmanagementsysteme einsetzen, resultiert dies vor allem aus dem nicht wahrgenommenen Nutzen. Zu hohe Kosten bzw. zu geringes Know-how sind hingegen keine ausschlaggebenden Gründe. Bei den Unternehmen, die IMS nutzen, wird als Folge eine höhere Sicherheit wahrgenommen sowie in begrenztem Maße strukturiertere Prozesse im Unternehmen. Wenig spürbar sei allerdings eine Reduktion der Ausfallzeiten, die Identifizierungsprobleme am Rechner i.d.R. verursachen – ein bislang gern genanntes Argument für den Einsatz von IMS. Die Erfüllung gesetzlicher Anforderungen wird nur in einzelnen Branchen wie dem Bank- und Versicherungsgewerbe als relevant eingestuft.

Für die baden-württembergischen IT-Unternehmen bedeutet dies, dass angesichts der steigenden Bedeutung des Themas Identitätsmanagement noch signifikante Spielräume bestehen. Gleichzeitig aber muss der Nutzen deutlich kommuniziert werden und es ist mit einer durchaus starken Zurückhaltung von Seiten der Unternehmen zu rechnen.

3. Gebäudesicherheit durch IT – Fallstudie anhand des Flughafens Stuttgart[4]

Der Flugverkehr boomt – in Baden-Württemberg, Europa und weltweit. Mit stetig zunehmenden Passagierzahlen steigen auch die Anforderungen an die Flughäfen. Eine verlässliche Infrastruktur am Boden ist Grundvoraussetzung dafür, dass der private wie geschäftliche Flugverkehr erfolgreich wachsen kann. Sicherheit ist dafür eine zwingende Bedingung. Spätestens seit den Anschlägen vom 11. September 2001 sind Flughäfen diejenigen öffentlichen Räume, an denen Sicherheitskonzepte ihre Tauglichkeit beweisen müssen, und an denen Sicherheitslücken fatale Folgen haben können. Die Bedrohungslage durch Terrorismus liegt in Deutschland bei einem Mittelwert im europäischen Vergleich. Andere Länder – vor allem Großbritannien – sind deutlich stärker gefährdet. Dennoch besitzt das Thema Sicherheit an Flughäfen eine hohe Relevanz für Deutschland – und ebenso entsprechende IT-basierte Sicherheitslösungen. Deutschland verfügt über eine Vielzahl von internationalen Verkehrsflughäfen und damit über eine hohe Zahl an Bedarfsträgern in diesem Bereich. Tabelle 1 gibt einen Überblick über die zehn größten Flughäfen in Deutschland, gemessen an den Passagierzahlen.

Tabelle 1: Rangfolge der Flughäfen in Deutschland nach Passagierzahlen 2007

Rang	Flughafen	Passagierzahl 2007
1.	Flughafen Frankfurt (FRA)	53.892.993
2.	Flughafen München (MUC)	33.893.160
3.	Flughafen Berlin (TXL/SXF/THF)	20.008.703
4.	Flughafen Düsseldorf (DUS)	17.805.122
5.	Flughafen Hamburg (HAM)	12.706.250
6.	Flughafen Köln/Bonn (CGN)	10.414.814
7.	**Flughafen Stuttgart (STR)**	**10.292.674**
8.	Flughafen Hannover (HAJ)	5.609.206
9.	Flughafen Nürnberg (NUE)	4.212.440
10.	Flughafen Hahn (HHN)	3.955.661

Quelle: Verkehrszahlenstatistik des ADV und Pressemeldungen der Flughäfen

Ein Flughafen eignet sich hervorragend als Fallstudie, um das Thema Sicherheit durch IT im öffentlichen Raum zu illustrieren. Flughäfen weisen sehr verschiedene Areale auf, die unterschiedlichen Sicherheitsstufen unterliegen und für die die Zugangsberechtigungen strikt geregelt sind, deren Einhaltung aber ebenso stetig überwacht werden muss. Der Eintritt einer Person in ein höher gesichertes Areal des Flughafens ohne eine entsprechende Zugangsberechti-

[4] Diese Fallstudie wurde erstellt von Bernd Hartmann. Der Autor dankt dafür den Mitarbeitern der Flughafen Stuttgart GmbH, die dies ermöglicht haben durch Bereitstellung von Informationen und die teilnehmende Beobachtung in der Leitstelle, insbesondere Dirk Spengler, Hans Wegerer, René Fischer und Peter Holl.

gung stellt eine Gefährdung der Sicherheit dar. Gleichzeitig sind verschiedene Akteure am Flughafen für die Einhaltung der Sicherheit zuständig, neben dem Flughafensicherheitspersonal auch die Bundespolizei oder die Feuerwehr. Diese Akteure müssen optimal untereinander abgestimmt arbeiten, um Sicherheit am Flughafen zu gewährleisten. Neben den Akteuren müssen aber auch die einzelnen Sicherheitssysteme am Flughafen bestmöglichst untereinander vernetzt sein, um keine Lücke im Sicherheitssystem entstehen zu lassen. Zur Koordination der verschiedenen Sicherheitsaspekte werden IT-basierte Endgeräte eingesetzt, die ebenfalls Innovationszyklen unterliegen und kontinuierlich angepasst werden an die aktuellen Bedürfnisse – sowohl der Sicherheit als auch der Bedienbarkeit. All dies sind Anforderungen, die gültig sind für jegliche Art von Gebäudesicherheit – an einem Flughafen aber in besonders intensiver Ausprägung.

Der Flughafen Stuttgart – Rahmendaten

Für die Fallstudie zum Thema „Sicherheit durch IT im öffentlichen Raum“ wurde der Flughafen Stuttgart ausgewählt. Der Flughafen Stuttgart ist als Flughafen von mittlerer Größe flächenmäßig der kleinste international agierende Flughafen Deutschlands. Die Geschichte des Flughafens reicht bis in die Vorkriegszeit zurück. Nach ersten Flugstarts auf dem Gelände des Cannstatter Wasens existierte der erste reguläre Flughafen ab 1925 in Böblingen-Hulb. Seit 1936 ist der Flughafen in Leinfelden-Echterdingen auf den Fildern angesiedelt (vgl. Abbildung 16).

Abbildung 16: Der Flughafen Stuttgart aus der Vogelperspektive

Quelle: Flughafen Stuttgart GmbH

In den 1960ern existierten Pläne, den Flughafen Stuttgart zu einem internationalen Großflughafen umzubauen, die jedoch nicht realisiert wurden. Heute besitzt der Flughafen Stuttgart vier Terminals, von denen Terminal 3 das neueste und größte ist und seit 2004 existiert. Ein ehemaliger Hangar wurde im Jahr 2000 ebenfalls in das heutige Terminal 4 umgebaut – von hier aus starten vor allem türkische Chartermaschinen.

Der Flughafen Stuttgart ist ein bedeutender Arbeitgeber in der Region: 9.500 Beschäftigte arbeiten in insgesamt rund 250 Unternehmen am Standort. Im Jahr 2006 wurde der Flughafen von 10,1 Millionen Passagieren frequentiert. Insgesamt 69 Airlines nutzen den Flughafen Stuttgart. Vom Flughafen Stuttgart aus sind 125 Ziele in 33 Ländern weltweit erreichbar. In 2006 erzielte der Flughafen Stuttgart einen Umsatz in Höhe von 211 Millionen Euro, bei einem Gewinn von 25,7 Millionen Euro. Mit diesen Angestelltenzahlen sowie Umsätzen ist der Flughafen Stuttgart in der Region eine wirtschaftlich treibende Kraft. Der Flughafen Stuttgart ist der Landesflughafen von Baden-Württemberg.

Methodik

Die Fallstudie wurde im Wesentlichen durch eine teilnehmende Beobachtung in der Leitstelle des Flughafens Stuttgart durchgeführt. Die hier gewonnenen Einsichten und Erkenntnisse wurden in anschließenden Interviews vertieft und inhaltlich abgesichert. Die Methode der teilnehmenden Beobachtung zeichnet sich durch die persönliche Teilnahme des Forschers an den Interaktionen der Personen, die das Forschungsobjekt sind, aus. Die teilnehmende Beobachtung kommt im deutschen Sprachraum seltener zur Anwendung als im anglo-amerikanischen Sprachraum, dennoch sprechen die Vorzüge der Methode für einen Einsatz. Durch die Teilnahme bzw. die unmittelbare Erfahrung der Situation werden Aspekte des Handelns und Denkens beobachtbar, die vergleichsweise in Gesprächen und Dokumenten über diese Interaktionen bzw. Situationen nicht zugänglich wären (vgl. Lüders 2003). Bei dieser Methode kann die Teilnahme je nachdem von bloßer physischer Präsenz bis zur vollständigen Interaktion mit eigener Rolle in der Gruppe reichen. Im Fall der teilnehmenden Beobachtung in der Leitstelle des Flughafens Stuttgart wurde die Beobachtung durch physische Präsenz durch ergänzende Fragen an das Personal der Leitstelle komplettiert.

Sicherheit und Sicherheitskonzepte

Sicherheit ist ein relativer Zustand, abhängig vom Risikopotenzial einer Situation. Bei komplexen Systemen ist es unmöglich, Risiken völlig auszuschließen. Anders ausgedrückt: „Sicherheit gibt es nicht – soviel ist sicher. Sicherheit ist ein Idealbild, die Vorstellung, dass zu keinem Zeitpunkt irgendwo etwas Gefährliches passieren kann. (...) Was man erreichen kann und so gut wie möglich sollte, ist ein umfassender Schutz vor Bedrohungen und ein weitestgehendes Abmildern der Folgen, wenn ein Unfall, ein Verbrechen oder eine Naturkatastrophe nicht verhindert werden konnte“ (Grasemann 2007b, S. 4).

Das vertretbare Risiko innerhalb eines Systems hängt von vielen Faktoren ab und ist angesichts des Nutzungskontextes unterschiedlich zu bewerten. Üblicherweise werden mit steigendem Nutzen eines Systems auch höhere Wahrscheinlichkeiten für Beeinträchtigungen als vertretbar angesehen. Ein solches Beispiel wäre die Teilnahme am Straßenverkehr – ein System, das bedeutende Gefährdungen aufweist, die sich nicht eliminieren lassen, dessen Nutzen aber deutlich überwiegt. Ist eine Situation erreicht, in denen das Gefährdungspotenzial einschätzbar ist und durch das eigene Verhalten möglichst gering gehalten wird, kann ein System als sicher gelten.

Im organisatorischen Kontext werden Sicherheitskonzepte erstellt und umgesetzt, um den Zustand von Sicherheit zu erreichen (vgl. Müller 2005). Ein Sicherheitskonzept stellt eine Analyse möglicher Angriffs- und Schadensszenarien dar, die das Ziel hat, zu einem definierten Schutzniveau zu gelangen. Sicherheitsmaßnahmen dienen dazu, dieses definierte Schutzniveau zu erreichen. Sicherheitsmaßnahmen sind erfolgreich, wenn sie dazu führen, dass mit ihnen sowohl erwartete als auch nicht erwartete Beeinträchtigungen abgewehrt bzw. hinreichend unwahrscheinlich gemacht werden.

Der Schutz im Rahmen des Sicherheitskonzeptes kann sich auf verschiedene Objekte beziehen, etwa den Schutz der öffentlichen Sicherheit, die Sicherheit der Mobilität, Sicherheit der Kommunikation, Sicherheit von Objekten oder Personen. Eine besondere Bedeutung gewinnt dabei entsprechend der amerikanischen Verwendung des Sicherheitsbegriffes die Sicherheit gegenüber böswilligen Angriffen („Security“) und die Sicherheit gegenüber menschlichem und technischem Versagen („Safety“). Entsprechend ist auch das Sicherheitskonzept am Flughafen Stuttgart in vier verschiedene Sicherheitsebenen unterteilt, je nachdem, was jeweils geschützt werden soll (vgl. Tabelle 2).

Tabelle 2: Ebenen der Sicherheit am Flughafen Stuttgart

Sicherheitsebene	**Geltungsbereich**
Flugsicherheit	Sicherheit von Mensch und Material bei Starts und Landungen von Flugzeugen
Security	Schutz des Flughafenbereichs (Personen und Gebäude) vor böswilligen Angriffen
Safety	Schutz von Personen vor menschlichem und technischem Versagen, z.B. Brände und Unfälle
Arbeitssicherheit	Sicherheit des Personals des Flughafens bei der täglichen Arbeit; besonders relevant für die Arbeit auf dem Vorfeld

Für die Sicherheit auf den verschiedenen Sicherheitsebenen sind unterschiedliche Akteure verantwortlich. „Security“ wird etwa durch Wachpersonal, Landes- und Bundespolizei gewährleistet, während für „Safety“ etwa die Feuerwehr verantwortlich ist. Besonders relevant wird es daher, die Sicherheitsebenen untereinander zu koordinieren und in ein ganzheitliches Sicherheitskonzept einzubetten. Das Sicherheitskonzept wird durch eine Vielzahl innovativer Syste-

me im Verbund gewährleistet, die zunehmend auf IT-basierten Endgeräten aufbauen. Beispiele sind z.B. digitale Videoüberwachung oder digitaler Bündelfunk.

Seit dem Jahr 2001 setzt der Flughafen Stuttgart auf eine integrierte IT-Gesamtlösung zur Planung des Personaleinsatzes und der Bodenabfertigung und –logistik, das so genannte Stuttgart Airport Management System (AMS), das modular und offen für Erweiterungen ist. Angesichts des erhöhten Betriebsaufkommens und insgesamt vier Terminals wurde dies nötig. Dadurch werden auch die Mitarbeiter auf dem Vorfeld – d.h. der Rangier-, Abstell- und Abfertigungsfläche für die Flugzeuge am Flughafen – koordiniert, die mit mobilen Endgeräten mit WLAN-Anschluss ausgerüstet sind, in denen Aufträge und Abfertigungsverträge gespeichert sind. Dieses System dient vor allem der Effizienz des Personaleinsatzes am Flughafen und der betriebswirtschaftlichen Abrechnung der Aufträge, doch es berührt auch die Flugsicherheit ebenso wie die Arbeitssicherheit.

Für die weitere Betrachtung von „Sicherheit durch IT“ wurden die Bereiche Flugsicherheit und Arbeitssicherheit aus dieser Fallstudie ausgeklammert. Im Zentrum stehen vielmehr die Sicherheitsebenen „Security“ und „Safety“. Die Kombination beider Bereiche steht für Gebäudesicherheit im öffentlichen Raum. Hier sind vor allem IT-basierte Endgeräte gefordert, eine möglichst große Harmonisierung zwischen beiden Sicherheitsebenen zu erreichen.

Insbesondere zwischen den Sicherheitsdimensionen Security und Safety existieren Zielkonflikte. Am Beispiel von Fluchttüren wird dies deutlich: Eine „Safety“-Anforderung wäre hier die Gewährleistung eines möglichst gefahrlosen Flucht- und Rettungsweges für Betroffene beziehungsweise Hilfe leistende Kräfte, während Forderungen zur Vermeidung einer unberechtigten Nutzung der Tür im Normalbetrieb dem Bereich „Security“ zuzuordnen sind.

Dies sind Fragestellungen, die sich im Rahmen der Gebäudesicherheit bewegen. Gebäudesicherheit wurde als Fokus dieser Fallstudie gewählt, da sie auf andere Arten von öffentlichen Räumen wie auch auf Unternehmensgebäude übertragbar ist. Das Thema Gebäudesicherheit und IT ist von besonderem Interesse, da sich hier in den letzten Jahren bedeutende Entwicklungen ergeben haben. Ein Gebäude wird heute als ein Ort vieler Prozesse verstanden, die mit Hilfe der Informationstechnologie optimiert und synergetisch verbunden werden können. Ein modernes Gebäude beherbergt oft mehrere verschiedene Formen von Netzwerken, darunter Telekommunikation, Warnmeldeanlagen, Zutrittssysteme und auch Steuerungen für Licht, Klima oder Beschattung. Durch die verschiedenen Netzwerke werden Prozesse kommunikationsfähig gemacht, was neben einer Steigerung der Leistungsfähigkeit und Zuverlässigkeit auch neue Funktionen ermöglicht.

Die Technologie, auf der die verschiedenen Netzwerke in einem Gebäude beruhen, ist bislang jedoch heterogen und spezialisiert. Entsprechend ist ein Netzwerk für Brandmelder anders aufgebaut als eines zur Übertragung von Videoströmen. Gegenwärtig vollzieht sich im Rahmen der Gebäudeautomation ein großer Entwicklungsschritt hin zum „integrierten Gebäude", der Konvergenz und Verbindung bislang getrennter Systeme (vgl. Palensky et. al. 2006).

Ein Beispiel für diesen Wandel zum integrierten Gebäude lässt sich am Gebäudemanagement des Landeskriminalamts Baden-Württemberg (LKA) studieren. Das Landeskriminalamt Baden-Württemberg (LKA) wurde im Jahr 1978 bezogen und umfasst vier Gebäude, die vor allem aus Bürobereich bestehen, aber auch Labore beherbergen. Im Laufe der Jahre haben sich die Anforderungen an die Gebäudetechnik vielfach verändert, etwa wurde durch eine veränderte Gebäudeautomation ein deutlich geringerer Energieverbrauch erzielt. So versammelten sich im Zuge diverser Sanierungsmaßnahmen sehr unterschiedliche Systeme zur Gebäudeautomation. Gegen Ende der 1990er Jahre wurde im Zuge eines erneuten Modernisierungsschubes damit begonnen, eine einheitliche Gebäudeleittechnik aufzusetzen, die die bisherigen Systeme integriert und offen ist für Erweiterungen. So wurde auf der existierenden Netzwerktechnologie auch ein neues Digitales Videomanagement System (DVS) im Rahmen der Gebäudesicherheit aufgesetzt (vgl. Haller 2005, S. 59). Dieser Entwicklungsschritt wird auch am Flughafen Stuttgart jetzt und in den noch kommenden Jahren vollzogen.

Das „integrierte Gebäude“ verspricht ein einfacheres Netzwerkmanagement, durchgängige Funktionen und die potenzielle Chance, vormals unabhängig betriebene Prozesse sinnvoll zu verbinden. Dennoch ist die Vernetzung der einzelnen Sicherheitssysteme eine bleibende Herausforderung. Insbesondere steigt auch durch die Konvergenz und die zahlenmäßig stetige Zunahme von Sensoren das Datenvolumen und die Systeme werden immer komplexer. Dadurch sind neue Konzepte hinsichtlich Anwendung, Integration, Implementierung und Wartung der Gebäudesicherheitssysteme erforderlich.

Einige Zahlen sollen dazu dienen, die bereits heute existierende Komplexität zu verdeutlichen. So sind im Areal des Flughafens Stuttgart heute rund 15.000 Brandmelder im Einsatz. Dazu existieren im Flughafenareal insgesamt rund 400 Türen mit Zutrittskontrollen. Ein Digitales Videomanagement System (DVS) verwaltet Bilder von über 100 Kameras. Dabei fallen über 1 Terrabyte Daten im Alarmspeicher an, der mehrere Wochen zurückreicht. Ein Alarmspeicher speichert Alarmauslösungen und Störungen auch nachdem der Störfall vorüber ist und im Bedarfsfall auch noch später ausgelesen werden kann – sollte sich etwa zeigen, dass ein Störfall strafrechtliche Folgen hat. Diese Zahlen verdeutlichen, dass ein handhabbares IT-gestütztes Gesamtsystem erforderlich ist.

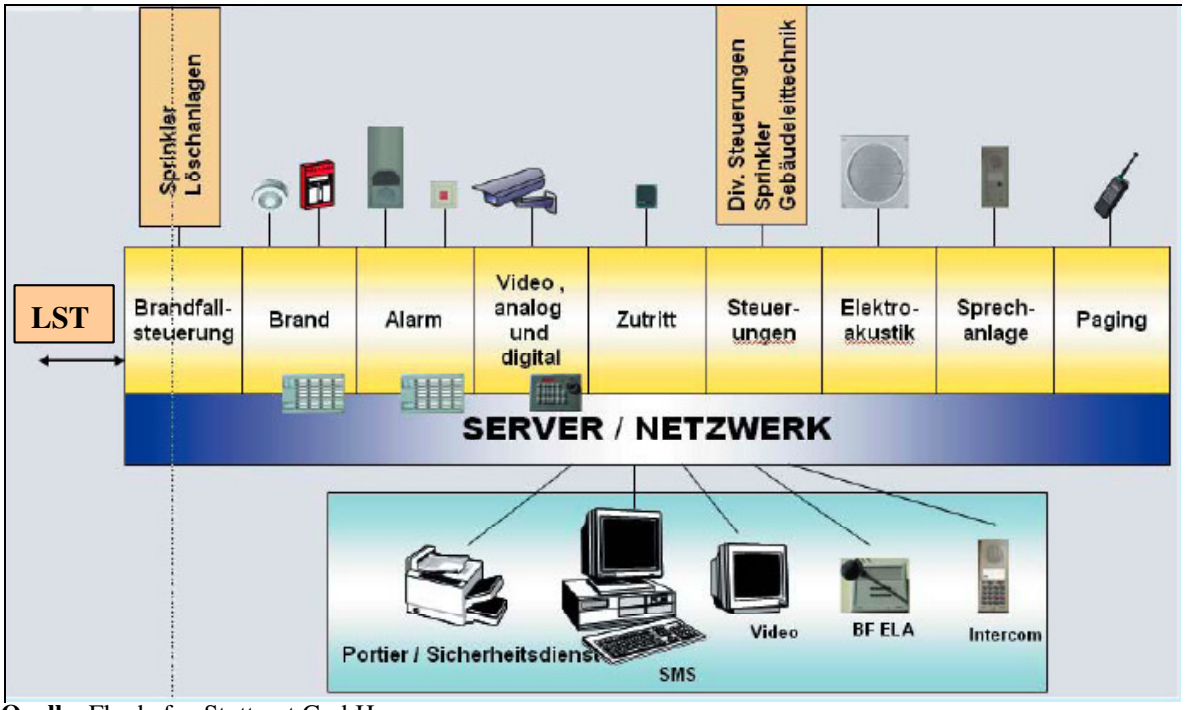
Die Leitstelle des Flughafens

Die verschiedenen Säulen des Sicherheitskonzeptes fließen in der Leitstelle zusammen. Hinter einer unscheinbaren Tür, die durch mehrfache Zugangsbeschränkungen gesichert ist, liegt dieses Herz des Flughafens. Hier arbeiten Flughafen- und Sicherheitsdienste Hand in Hand. Zahlreiche Bildschirme zeigen verschiedene Bereiche des Flughafens, hier erscheinen Alarme, und das Digitale Videoüberwachungssystem ist im Einsatz. Die Leitstelle ist rund um die Uhr besetzt. Lediglich nachts von 23 Uhr bis 4 Uhr morgens ist es mit geringerer Personenzahl besetzt, wenn aufgrund Nachtflugbeschränkung weniger Betrieb herrscht. Die verschiedenen Sicherheitssysteme am Flughafen werden von hier aus bedient und überwacht und in einem zen-

tralen Safety Management System (SMS) zusammengefasst. Mithilfe eines automatisierten Alarmiersystems wird hier die Sicherheit am Flughafen gewährleistet. Gemeinsame Standards und offene Schnittstellen sorgen für einen reibungslosen Datenfluss.

Abbildung 17 gibt einen Überblick über die technischen Einzelsysteme und Netzwerke, die in der Leitstelle Sicherheit und Technik (LST) des Flughafens gesteuert werden.

Abbildung 17: Sicherheitsrelevante Einzelsysteme unter Kontrolle durch die Leitstelle



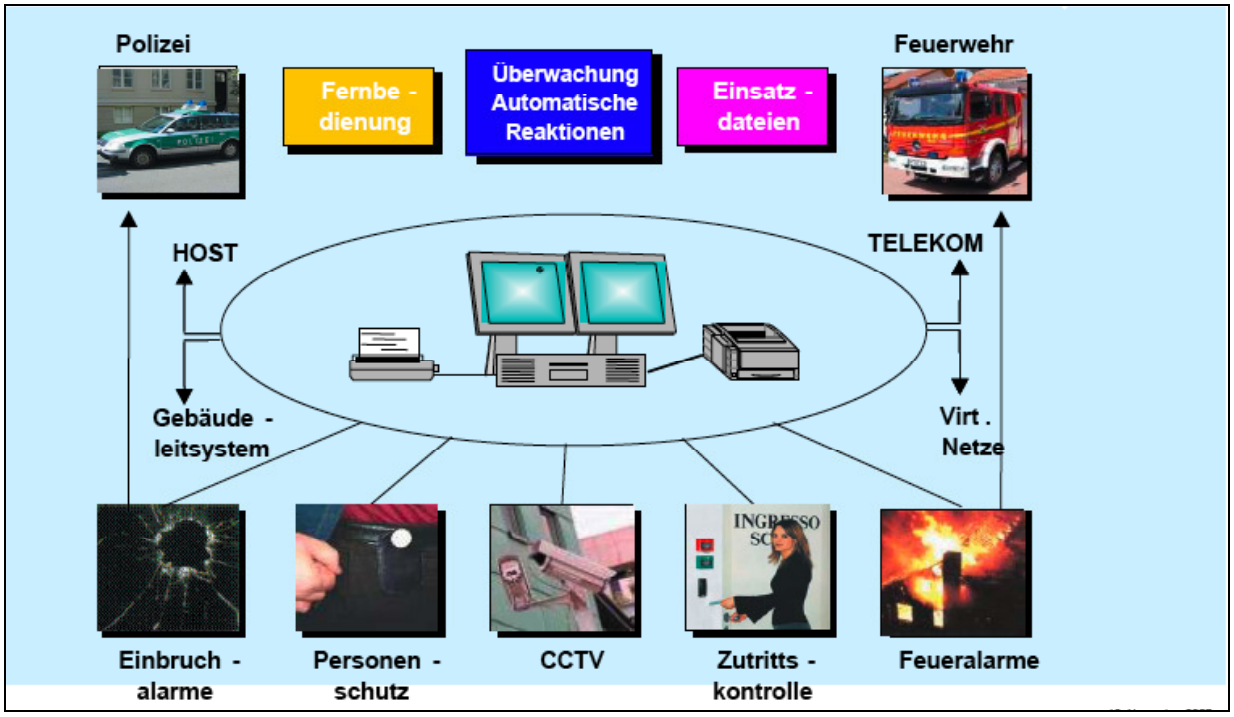
Quelle: Flughafen Stuttgart GmbH

Eine zentrale Rolle im Rahmen der Gebäudesicherheit spielt das Tür-Management. Insgesamt mehr als 400 Türen mit Zutrittskontrollen im Flughafenareal werden von der Leitstelle aus überwacht. Türen mit Zutrittskontrollen liegen besonders an den Übergängen zwischen verschiedenen Bereichen mit unterschiedlichen Sicherheitsstufen und trennen die sensiblen Bereiche ab. Die Zuweisung der Zutrittsrechte zu den einzelnen Sicherheitsarealen ist auf verschiedenen Stufen geregelt. Wo früher reine Schlüsselsysteme eingesetzt wurden, steht heute eine Kombination aus Schlüsseln und Chipkarten, in die die Berechtigungen einkodiert werden.

Die Dauer des Offenstehens dieser Türen ist kurz, jede Verlängerung führt zu einem Alarm im SMS. Ein Wachmann wird automatisch darüber informiert. Auch bei Schleusen, durch die die ankommenden Fluggäste in den öffentlichen Gebäudebereich übertreten, existieren Beschränkungen: Ein Durchgehen ist nur in eine Richtung möglich. Gehen Personen wieder zurück, wird dies durch Sensoren erfasst und ebenfalls ein Alarm ausgelöst. Gleichzeitig erscheint die entsprechende Tür oder Schleuse, an der der Alarm ausgelöst wurde, auf dem Bildschirm in der Leitstelle. Im Idealfall wäre dieser Bildschirm also immer schwarz, da dies bedeutet, dass kein Störfall vorliegt. In der Realität werden hier mehrmals pro Stunde Störfälle angezeigt. Das An-

zeigen des Störfalls geht einher mit einem akustischen Warnsignal in der Leitstelle, die das technische Personal auf den Störfall aufmerksam macht. In den meisten Fällen sind dies unproblematische Störfälle – etwa wenn eine Tür nicht richtig schließt. An der Tür selbst wird ebenfalls ein Alarm angezeigt. Ein paar Zahlen dazu: von 16.868 Störfällen im Jahr 2006 wurden 4.933 weitergemeldet, z.B. an die Polizei oder Feuerwehr. Dementsprechend handelt es sich bei deutlich mehr als zwei Drittel der Störfälle um rein technische Störungen. Die Störfälle werden vom Disponenten in der Leitstelle Tag und Nacht überwacht, protokolliert und im Ernstfall an die entsprechenden Stellen weitergeleitet.

Abbildung 18: Vernetzung im Rahmen des Sicherheitskonzepts am Flughafen Stuttgart



Quelle: Flughafen Stuttgart GmbH

Anforderungen an Sicherheitssysteme

Die Anforderungen an die Sicherheitssysteme in der Leitstelle werden sowohl aus der Unternehmensumgebung (externe Anforderungen) wie auch von innerhalb des Unternehmens selbst (interne Anforderungen) erzeugt. Bei den externen Anforderungen handelt es sich vorrangig um regulatorische Neuerungen, wie etwa EU-Richtlinien, DIN-Spezifikationen oder versicherungstechnische Forderungen. Die internen Anforderungen entstehen hingegen aus der täglichen Arbeitspraxis in der Leitstelle und im Flughafenareal und werden durch die beteiligten Mitarbeiter in die Innovationsprozesse eingespeist. Im Wechselspiel der externen und internen Anforderungen werden Entscheidungen für bestimmte Systemlösungen getroffen. Im Folgenden werden die externen und internen Anforderungen näher erläutert.

Externe Anforderungen an Sicherheitssysteme

Die Anforderungen an die Gebäudesicherheit, die von extern an den Flughafen herangetragen werden, bestehen vor allem aus klaren gesetzlichen und regulatorischen Auflagen. Gehört ein Flughafen bereits jetzt zu den Gebäuden, für die mit die schärfsten Sicherheitsauflagen gelten, ist schon abzusehen, dass der Flughafen von morgen ein noch strenger gesicherter Bereich sein wird als heute. Im Flugverkehr kommt durch das Thema Mobilität verstärkt europäisches und internationales Recht zum Greifen; EU-Richtlinien werden dann in nationales Recht umgesetzt. Zum Jahresbeginn 2006 hat die EU-Kommission auch die für Flughäfen gültigen Sicherheitsbestimmungen erneut verschärft. Danach sind zum Beispiel für Mitarbeiter der Flughäfen Personenkontrollen verpflichtend. Zudem fordert die EU-Kommission nun auch die strikte Trennung von sieben verschiedenen Passagierströmen im Flughafenareal: incoming, outgoing, transfer, EU, Non-EU, Schengen, Non-Schengen. Damit einher gehen schließlich auch neue Anforderungen an das Sicherheitskonzept und die Arbeit in der Leitstelle.

Weitere externe Anforderungen mit Auswirkungen auf das Sicherheitskonzept des Flughafens entstehen aus versicherungstechnischen Auflagen, insbesondere im Bereich des Brandschutzes. Der Flughafen muss die Forderungen des Verbandes der Sachversicherer erfüllen, um Versicherungsleistungen empfangen zu können. Dies wiederum hat Auswirkungen auf die Ausstattung der Leitstelle, da bestimmte technische Systeme wie etwa ein Gefahrenmeldesystem und eine Dokumentation der Störungen gefordert werden. Auch wo diese Forderungen nicht unbedingt gesetzlich vorgeschrieben sind, hat der Flughafen ein Interesse daran, diese zu erfüllen, um nicht in eine höhere Versicherungsstufe eingeordnet zu werden.

Interne Anforderungen an Sicherheitssysteme

Obgleich zahlreiche Funktionen der Leitstelle durch externe Anforderungen initiiert werden, wird deren konkrete Ausgestaltung doch deutlich durch die Anforderungen der Mitarbeiter beeinflusst. Die möglichst einfache Bedienbarkeit und möglichst hohe Nutzerfreundlichkeit der Sicherheitssysteme ist daher eine Hauptanforderung an jegliche neue Sicherheitstechnologie, die in der Leitstelle des Flughafens Stuttgart eingesetzt werden sollen. Durch die zahlreichen Alarme und eingehenden visuellen wie akustischen Informationen müssen sich Sicherheitssysteme auch durch wohldurchdachte Informationsverarbeitung auszeichnen. Hinzu kommen Anforderungen an die bauliche Verwendbarkeit der Systeme: Sie müssen sich durch ihre Größe und Formgebung leicht für einen Einbau in die existierenden Armaturen der Leitstelle eignen. Durch den 24-Stunden-Betrieb an einem Ort, an dem die Sicherheitsüberwachung keinen Moment ausfallen darf, ist schließlich auch die Zuverlässigkeit im Einsatz eine wesentliche Anforderung an die Komponenten des Sicherheitssystems.

Ein Beispiel ist etwa ein vom Verband der Sachversicherer vorgeschriebenes normiertes Kopfteil, über das Störungen registriert werden. Dieses ist in der Leitstelle vorhanden und muss auch funktionieren. Gearbeitet wird im Regelfall jedoch von einem anderen Arbeitsplatz aus, auf den die Funktionen des Norm-Kopfteils aufgeschaltet werden. Dies ist eine Folge des Bedürfnisses an besserer Bedienbarkeit durch die Mitarbeiter.

Innovationszyklen der Sicherheitstechnologie in der Leitstelle

Aufgrund technologischen Wandels hat sich das Gesicht der Leitstelle des Flughafens Stuttgart innerhalb der letzten 20 Jahre stark gewandelt. Es handelt sich dabei jedoch um einen schleichenden Wandel, bei dem einzelne Elemente nach und nach ausgetauscht oder erweitert werden, während existierende Elemente weiterhin im Einsatz bleiben. Die Zahl der Monitore ist dabei ständig gewachsen, und es hat sich eine erhebliche Anzahl unterschiedlicher Anlagetypen in der Leitstelle angesammelt. Die Innovationszyklen innerhalb der Leistelle sind somit nicht durch klare Brüche gekennzeichnet, sondern weisen einen graduellen Austauschprozess einzelner Elemente auf, der sich über Jahre hinzieht. Das Alter einzelner Systeme in der Leitstelle beträgt zum Teil zehn Jahre, jedoch ist dies nur dadurch möglich, dass sie gut zu aktualisieren sind. Neuere Systeme müssen auch mit deutlich älteren noch interagieren können. Dadurch, dass im Laufe der Zeit die vorhandenen Systeme weiter ausgebaut wurden und neue hinzukamen, ist jedoch auch die technische Ausrüstung immer komplexer und zunehmend unüberschaubar geworden.

Neben der zunehmenden Ausdehnung der technischen Geräte innerhalb der Leitstelle sind gleichzeitig auch die Systeme immer komplexer geworden. Dies stellt neue Anforderungen an das Personal, das in der Leitstelle arbeitet. Während etwa vor 20 Jahren die Zahl und Größe der technischen Systeme in der Leitstelle noch wesentlich geringer war, war gleichzeitig das Team deutlich größer. Zahlreiche Aufgaben wurden seitdem automatisiert. Eine kleinere Zahl an Mitarbeitern muss also heute deutlich komplexere Systeme bedienen, die immer höheren Anforderungen genüge tun. Neben einem dafür erforderlichen höheren Bildungsgrad der Mitarbeiter ist dadurch auch der Schulungsaufwand deutlich gestiegen.

Der Wandel der Arbeitswelt in der Leitstelle durch IT zeigt sich auch am Bereitschaftsdienst der Techniker. Wenn bei Nacht Störmeldungen anfielen, musste der Techniker zugegen sein und wurde per Piepser oder Telefon verständigt. Heute kann der Techniker im Bereitschaftsdienst nach Hause gehen und kann sich von dort aus über einen Laptop in das Stör-Management-System der Leitstelle einloggen. Er kann dann fallweise entscheiden, ob der Störfall seine umgehende Präsenz erfordert oder ob die Behebung des Störfalls auch noch am nächsten Morgen erfolgen kann. Hier führt IT zu einer flexibleren Gestaltung des Arbeitseinsatzes und letztlich zu mehr Effizienz in der Ressourcenallokation.

Bereits jetzt ist am Flughafen Stuttgart das nächste Etappenziel für die kommenden Jahre erkennbar: ein einheitliches Kopfsystem in der Leitstelle, in dem sämtliche Einzelsysteme integriert sind. Es existiert nur noch ein Arbeitsplatz, von dem aus der Mitarbeiter sämtliche Möglichkeiten der Leitstelle nach Belieben zur Verfügung hat. Je nach aktueller Situation kann er sich die benötigten Module an den Arbeitsplatz zuweisen, und es gibt nur einen Monitor, auf dem alle im Moment benötigten Informationen angezeigt werden. Bereits heute lässt sich diese Entwicklung in anderen Leitstellen beobachten, etwa am Flughafen Frankfurt.

Es ist bereits abzusehen, dass die Sicherheitsanforderungen an Flughäfen in den nächsten zehn Jahren weiter steigen werden. Dies ist eine Folge des erhöhten Verkehrsaufkommens sowohl im Güter- wie auch Personenverkehr. Megatrends wie die Globalisierung der Wirtschaft und die zunehmende Mobilität aller Schichten der Bevölkerung sind dafür bedingende Faktoren. Gleichzeitig bringt dies weiter steigende Bedrohungen der Sicherheit auf allen Ebenen mit sich, von der Flug- über die Arbeitssicherheit bis zu Security und Safety. Neue externe Anforderungen werden die Folge sein, die wiederum weitere Systemelemente in der Leitstelle erfordern. Vor diesem Hintergrund ist die integrierte Leitstelle aus Sicht der internen Anforderungen eine unbedingte Notwendigkeit, um mit einem gestiegenen Maß an Komplexität der technischen Systeme noch so umgehen zu können, dass es vom Personal gehandhabt werden kann.

Die internen Anforderungen an die Sicherheitssysteme spielen dementsprechend auch eine herausragende Rolle im Innovationsprozess der Technologie innerhalb der Leitstelle. Kenntnisse über Innovationen und effiziente neue Systeme werden durch die in der Leitstelle des Flughafens Stuttgart direkt arbeitenden Mitarbeiter innerhalb der Hierarchie nach oben getragen. Die Mitarbeiter besuchen regelmäßig andere Leitstellen in Deutschland sowie Fachmessen und -kongresse. Entsprechend können die Mitarbeiter der Leitstelle selber als IT-Experten auf ihrem Gebiet gelten und spielen eine gewichtige Rolle bei Einkaufsprozessen neuer Systemkomponenten.

Eine besondere Rolle im Innovationsprozess spielen auch „Teststellungen“ neuer Technologien und Systeme innerhalb der Leitstelle des Flughafens Stuttgart wie auch anderen Leitstellen bundesweit. Häufig werden so verschiedene Anbieter eines Systems im Einsatz getestet, bevor eine Kaufentscheidung getroffen wird. Aufgrund der Situation von Flughäfen als Gebäude mit einem starken Sicherheitsbedarf und reibungslosen Abläufen sind die Leitstellen interessante Referenzkunden für die Industrie. Gleichzeitig sind Flughäfen als Organisationen höchst aufgeschlossen für neue Technologien. Entsprechend werden Teststellungen neuer Systeme für Zeiträume von vier Wochen bis zu einem Jahr in der Leitstelle bereitgestellt. Hier können diese dann bei Zufriedenheit mit dem System von den Mitarbeitern anderer Flughäfen – aber auch anderer Organisationen mit einem hohen Sicherheitsbedarf – in Augenschein genommen werden, z.B. die Bundesbank, Pharmakonzerne oder Automobilhersteller. Was am Flughafen Stuttgart funktioniert, kann auch für Daimler interessant sein. Im selben Maße suchen auch die Mitarbeiter der Leitstelle des Flughafens Stuttgart andere Leitstellen auf, um Teststellungen im Einsatz zu erleben.

Ein aktuelles Beispiel für den Test einer Sicherheitstechnologie ist der Test verschiedener Systeme der Zutrittskontrolle mittels biometrischer Merkmale am Flughafen Stuttgart. Zum Einsatz kamen Systeme zur biometrischen Erkennung von Gesichtern, Fingerspitze, Handgeometrie, 2-Fingergeometrie, Iriserkennung, oder der Stimme-Lippe-Kombination. Das Ergebnis war jedoch, dass bislang keines dieser Systeme für den Dauereinsatz oder für größere Benutzergruppen geeignet ist. Lediglich für kleinere Gruppen, die sich auf spezifische Gegebenheiten und notwendige Verhaltensweisen einstellen können und wollen, mag diese Technologie aus Sicht des Flughafens Stuttgart bereits tauglich sein. Auf biometrische Sicherheitstechno-

logien treffen noch nicht die internen Anforderungen zu, nämlich baulich verwendbar, leicht zu bedienen und zuverlässig im Einsatz zu sein.

Weitere Zukunftstechnologien wie RFID im Gepäcktracking oder softwarebasierte Bildanalysen im Digitalen Videomanagement-System zur Identifizierung von potenziellen Bedrohungen werden kontinuierlich untersucht. Dabei bleibt festzuhalten, dass Sicherheit keine Frage der Kosten ist. Hauptkriterium für die Auswahl eines neuen Sicherheitssystems ist, dass dadurch die Sicherheit deutlich gesteigert wird und das System einfach zu bedienen und zuverlässig im Einsatz ist. Gerade vor dem Hintergrund von externen Anforderungen sind Kosten nicht unbedingt das Hauptauswahlkriterium beim Einkauf neuer Systeme. Sicherheitssysteme sind aus Sicht des Controlling eigentlich immer zu teuer, da sie Geld kosten und kein Geld einbringen. Dennoch ist auf einer höheren Ebene Sicherheit die elementare Grundvoraussetzung für das Funktionieren des Geschäftsmodells Flughafen überhaupt. Dementsprechend werden auch weiterhin neue Technologien und Systeme aufmerksam von der Leitstelle des Flughafens Stuttgart beobachtet, analysiert und auf ihre Relevanz für den Flughafen hin bewertet.

Gebäudesicherheit als Chance für KMU

Für mittelständische Unternehmen bieten sich beim Thema „Gebäudesicherheit durch IT“ verschiedene Marktchancen. Dies erfordert jedoch einen langen Atem, Beharrlichkeit und eine Bereitschaft, sich auf öffentliche Vergabeverfahren einzulassen. Im Bereich der Informations-, Kommunikations- und Sicherheitstechnologien haben regionale Unternehmen aus Baden-Württemberg erstklassige Kompetenzen und ausgeprägte Erfahrungen zu bieten. Insbesondere die Integration diverser Netzwerke innerhalb eines Gebäudes und die Schaffung von IT-Gesamtlösungen für die unterschiedlichsten Prozesse und Arbeitsabläufe auf einem Flughafen erfordert Expertise.

Gerade ein regional stark verwurzeltes Unternehmen wie der Flughafen Stuttgart schätzt das Know-How von IT-Produzenten und Dienstleistern vor Ort, die die Abläufe und die Lokalität kennen und auch schnell zur Stelle sind. Entsprechend kommen zahlreiche der Sicherheitstechnologien in der Leitstelle von baden-württembergischen Unternehmen oder werden durch baden-württembergische Filialen von Unternehmen betreut.

Die Situation der Anbieter von Sicherheitstechnologien mit Sitz in Baden-Württemberg wird daher aus Sicht der Leitstelle sehr positiv beurteilt. Mit Niederlassungen von Bosch oder Siemens, die sich direkt mit Gebäudetechnik und Sicherheitssystemen befassen, ist die Kompetenz großer Konzerne im Land, gleichzeitig existieren viele spezialisierte Firmen für einzelne Sicherheitstechnologien. Mit Firmen wie etwa Vitracom (Karlsruhe), VISENSO (Stuttgart) oder Securiton (Achern), Telenot (Aalen) oder eyevis (Reutlingen) gibt es in Baden-Württemberg Spezialisten für verschiedene Sicherheitstechnologien insbesondere im Bereich Visualisierung, Videoüberwachung und Großbildsysteme.

Angesichts immer höherer Sicherheitsanforderungen und komplexen Gefährdungssituationen kommt in der Zukunft integrierten Sicherheitsleitsystemen eine große Bedeutung bei, d.h. Systeme, die Informationen aus sehr heterogenen und verteilten Quellen schnell verarbeiten können. Dabei sind sowohl stationäre als auch mobile Quellen im Einsatz. Auf diesem Gebiet liegen auch bedeutende Chancen für neue Produkte und Dienstleistungen – gleichzeitig aber erfordern Innovationen hier auch die Kooperation verschiedener Akteure mit ihrem Spezialwissen.

Aus Sicht der Anforderungen gilt es für KMU, sowohl die externen als auch die internen Anforderungen permanent zu überwachen. Dazu gehört eine andauernde Beobachtung der Entwicklungen auf europäischer Ebene und eine Analyse der Auswirkungen auf potenzielle Kunden. Angesichts der Relevanz der internen Anforderungen ist es für Unternehmen, die Gebäudesicherheit als Marktchance nutzen wollen, ebenfalls wichtig, die aktuellen Bedürfnisse der Mitarbeiter zu kennen. Neben einer Präsenz auf den Leitmessen und Kongressen der Sicherheitsbranche[5] ist auch das Angebot von Teststellungen der eigenen Systeme nutzbringend, um Multiplikatoreneffekte zu erzielen. Letztendlich zählt im Vergabeverfahren immer das wirtschaftlichste Angebot. Dennoch ist insbesondere auch das Verhältnis von Wirtschaftlichkeit und technischer Leistungsfähigkeit des Systems ein wesentlicher Faktor. Die Mitarbeiter von Leitstellen können selber als IT-Experten gelten. Sie von den Vorzügen des eigenen Systems zu überzeugen ist sicherlich die größte Herausforderung – gleichzeitig ist dies die entscheidende Hürde, die jeder Hersteller von IT-basierten Sicherheitssystemen meistern muss.

Zusammenfassung und Ausblick

Diese Fallstudie zu Gebäudesicherheit durch IT anhand des Flughafens Stuttgart hat die Entscheidung für oder gegen bestimmte IT-basierte Sicherheitssysteme aus der Perspektive des Nutzers und Einkäufers der Technologien beleuchtet. Ein Akteur wie der Flughafen Stuttgart, bei dem Sicherheit die höchste Priorität hat, ist einer Reihe von externen und internen Anforderungen unterworfen, die gleichzeitig zu Treibern für Innovationszyklen im Bereich IT-basierter Sicherheitssysteme werden. Die letzten 20 Jahre haben das Gesicht der Leitstelle grundlegend verändert: Im Zuge des technologischen Wandels wurden zahlreiche Prozesse automatisiert, gleichzeitig sind auch die Anforderungen an das Bedienpersonal in der Leitstelle gestiegen. Die Innovationszyklen innerhalb der Leistelle sind jedoch nicht durch klare Brüche gekennzeichnet, sondern weisen einen graduellen Austauschprozess einzelner Elemente auf, der sich über Jahre hinzieht. Neuere Systeme müssen auch mit deutlich älteren noch interagieren können. Externe Anforderungen liegen in EU-Richtlinien, DIN-Normen oder von Seiten des Verbandes der Sachversicherer vor, interne Anforderungen werden aus der Perspektive der Nutzung und der Angemessenheit gestellt. So müssen die entsprechenden Systeme in die bisherige räumliche Situation integrierbar, nutzerfreundlich und zuverlässig im Einsatz sein. Im Wechselspiel zwischen externen und internen Anforderungen werden Entscheidungen für bestimmte Systemlösungen getroffen. Dabei sind die Kosten nicht unbedingt das Hauptauswahlkriterium

[5] Etwa die Leitmesse „Security“ in Essen, siehe http://www.security-messe.de

beim Thema Sicherheit; manchmal fällt die Entscheidung für Systeme, die betriebswirtschaftlich nicht vertretbar wären – aber nötig sind.

Diese Entwicklung hält unvermindert an: Flughäfen werden in Zukunft durch neue externe Anforderungen eher noch sicherere Gebäude, d.h. in der Leitstelle werden auch weiterhin neue Systemelemente hinzukommen. Entsprechend ist es das Ziel, eine integrierte Leitstelle mit einheitlichem Kopfsystem und maximal vier Bildschirmen einzurichten, auf die die verschiedenen Sicherheitselemente flexibel geschaltet werden können

Die Rolle der Mitarbeiter in den Innovationszyklen ist dabei hoch: Kenntnisse über Innovationen werden durch die in der Leitstelle direkt arbeitenden Mitarbeiter nach oben getragen. Die Mitarbeiter besuchen regelmäßig andere Leitstellen in Deutschland sowie Fachmessen und Kongresse; entsprechend müssen auch die Mitarbeiter der Leitstelle als Experten von innovativen neuen Systemen überzeugt sein. Im Falle von Biometrie und automatischen Bildanalysen ist diese Überzeugung im Hinblick auf das Kosten-Nutzen-Verhältnis noch nicht vorhanden, die Tests mit biometrischen Systemen konnten bislang nicht überzeugen.

Beschaffungsprozesse bieten gerade für Unternehmen vor Ort Geschäftschancen – wenn sie sich auf die besonderen Anforderungen von Sicherheit in öffentlichen Räumen einlassen. Insbesondere für KMU ist ein langer Atem nötig. Ein Flughafen kann jedoch ein hervorragender Referenzkunde sein, der auch weitere Kunden aus anderen Industrien überzeugt, bedingt durch die hohen Sicherheitsauflagen an Flughäfen. Entsprechend kann die Teststellung einer neuen Technologie hier attraktiv sein, da sich dadurch Multiplikatoreneffekte ergeben, die auch auf andere Industriekunden wie Banken oder Automobilhersteller ausstrahlen.

4. Sicherheit durch IT – Fünf Anwendungsszenarien für das Jahr 2020[6]

Gegenstand dieser Untersuchung sind informationstechnische Lösungen zur Erhöhung von Sicherheit in unterschiedlichen Anwendungsbereichen. Eine szenarioartige Darstellung zeigt die Potenziale insbesondere von Zugangs- und Überwachungstechnologien (digitale Signaturen, Smart Tags, Videoerkennungssysteme usw.) auf, indem sie mögliche Anwendungen im Jahr 2020 beschreibt. „Sicherheit" ist seit dem 11. September 2001 ein Thema, das vor allem im Zusammenhang mit öffentlicher Sicherheit und mit Sicherheit vor Terroranschlägen behandelt wird. Allerdings beinhaltet der Begriff weit mehr und hat ebenfalls eine wichtige Bedeutung im Bereich des Verkehrs, in den Unternehmen, beim Einkaufen über das Internet oder im Bereich der Medizin und der Gesundheit. Untersucht man diese Bereiche im Hinblick auf spezifische Anwendungspotenziale neuester Sicherheitstechnologien, so zeigt sich zum einen der bekannte Querschnittscharakter der Informationstechnik (IT) und zum anderen, welches Veränderungspotenzial in einem konsequenten und durchgehenden Einsatz dieser Technologien steckt. Die breitere Definition von Sicherheit, wie sie hier verwendet wird, ermöglicht es, aktuelle Entwicklungen, künftige Anwendungsbereiche und neue Märkte in den Blick zu nehmen, die für die Akteure in Baden-Württemberg von besonderer Bedeutung sind.

Dieses Kapitel gliedert sich in drei Teile: Zunächst geht es um die konzeptionelle Klärung des Sicherheitsbegriffs, anschließend werden Methode und Vorgehen erläutert und schließlich steht die ausführliche Darstellung der Bereiche öffentliche Sicherheit, Sicherheit im Verkehr, sicherer Zugang zum Unternehmen und zum Smart Home, sicheres Einkaufen im Internet sowie Sicherheit in Medizin und Gesundheit im Mittelpunkt. Die fünf Anwendungsszenarien sind als Diskussionsgrundlage gedacht; nicht immer sind die darin beschriebenen Entwicklungen wünschenswert, viele erscheinen vom heutigen Standpunkt aus gesellschaftlich nicht durchsetzbar, bei anderen dagegen fragt man sich, warum sie nicht längst im breiten Einsatz sind. In diesem Sinne will die Untersuchung Anregungen zur weiteren Diskussion bieten, die sich mit dem Einsatz von Erkennungs-, Zugangs- und Überwachungssystemen beschäftigt.

Welche Sicherheit ist gemeint?

Nimmt man den ganzen Bereich der Sicherheit durch IT in den Blick und beschränkt sich nicht auf terroristische Bedrohungen, so stößt man schnell auf die große Bedeutung der „zivilen Sicherheit". Störungen an neuralgischen Punkten (z.B. Trinkwasser- und Stromversorgungssysteme, Industrieanlagen, Kernkraftwerke oder Transport- und Telekommunikationsnetze) kön-

[6] Dieses Kapitel ist aus der Forschungsarbeit von Bernd Beckert und Kerstin Goluchowicz (beide Fraunhofer ISI) entstanden, die im Kontext von FAZIT-Forschung Szenarien für den IT- und Medienstandort Baden-Württemberg entwickelt haben. Im Laufe dieses Szenarioprozesses zeigte sich, dass „Sicherheit durch IT" ein bedeutendes Thema ist, dessen vielfältige Teilaspekte in eine separate Untersuchung zum Thema „Sicherheit durch IT" fließen sollten.

nen nämlich nicht nur durch Terroranschläge ausgelöst werden, sondern auch durch menschliches Versagen oder Naturkatastrophen. Niesing zählt in ihrem Aufsatz „Sicherheit durch High-Tech“ Beispiele auf, die diesen Sachverhalt illustrieren: „Selbstmordattentäter legen das Verkehrsnetz von London lahm, New Orleans versinkt fast in den Fluten, Viren, die das Schwere Akute Atemwegssyndrom (SARS) verursachen, gelangen über Flugzeuge innerhalb weniger Stunden rund um die Welt. Heute müssen wir uns vor terroristischen Angriffen, Industrieunfällen und Pandemien schützen. Gefragt ist nicht mehr nur militärische, sondern zunehmend zivile Sicherheit“ (Niesing 2007, S. 8).

In den hier entwickelten Anwendungsszenarien werden die heutigen Bedrohungssituationen in die Zukunft projiziert. Gleichzeitig werden Technologien, die heute noch in der Entwicklung sind, als funktionsfähig und einsetzbar gedacht, um ihre Anwendungsfelder und Auswirkungen in der Zukunft zu beschreiben.

Im Mittelpunkt stehen dabei *Zugangs- und Identifikationstechnologien*, die von der digitalen Videoüberwachung bis zu Biochips und Biosensoren reichen. Die Funktionsweisen und Potenziale dieser neuen Technologien werden in den einzelnen Anwendungsszenarien näher beschrieben. Einen Überblick über die betrachteten Technologien zeigt Tabelle 3.

Tabelle 3: Überblick über die betrachteten informationstechnischen Lösungen zur Erhöhung von Sicherheit

Technologie	*Beschreibung/ Beispiele*
Digitale Videoüberwachung	Erkennung von Personen, autonome „Verfolgung“ von Personen und Objekten, Erkennung von Bewegungsprofilen, Szeneninterpretation "intelligenter" Kameras
Identitätsmanagementsysteme	Automatische Vergabe von Zugangs- und Nutzungsrechten, Zugang zu arbeitsrelevanten Informationen zu jeder Zeit an jedem Ort, um knowledge-sharing und Koordination zu verbessern, rollenbasierte Systeme und Identitätsmanagement
Biometrische Sicherheitstechniken inkl. Bild- und Mustererkennungsverfahren	Fingerabdruck- und Handflächen-Scan, Irisscan, 3D-Gesichtserkennung, Sprach- und Sprechererkennung, Statur- und Gangerkennung, DNA-Scan
Chipkarten	z.B. Gesundheitskarte mit elektronischen Patientendaten
PINs und digitale Signaturen	PIN: Personal Identification Number, Chipkarten mit digitaler Signatur zur rechtskräftigen digitalen Unterschrift
Smart tags	RFID und elektronische Schlüssel, elektronische Label für Markenprodukte zur Unterscheidung von Fälschungen oder auch zur Sicherstellung der Unversehrtheit von Sendungen, „digitale Aura“
Verkehrsüberwachung	Fahrzeugassistenz- und Überwachungssysteme (Abstandshalter, Gefahrenerkennungssysteme, Einschlafverhinderung, automatische Assistenz- und Notfallalarmierung), Mautsysteme zur Überwachung
Datamining-Verfahren	Aufspüren verdächtiger Muster. Voraussetzung ist die Speicherung von Telefondaten, Bewegungsdaten, Kreditkarteneinsätzen, Flugdaten sowie die Online-Überwachung.
Biochips und Biosensoren	Mobiles Monitoring des aktuellen gesundheitlichen Zustands, inkl. Sensoren zum Aufspüren von Bakterien, Viren, Giftstoffen und Sprengstoffen

Idealerweise werden diese Zugangs-, Verschlüsselungs- und Identifikationstechnologien nicht im Sinne einer neuen Hermetik eingesetzt, die einen spontanen Umgang unmöglich macht und vor allem ausgrenzt, sondern umgekehrt als *Enabler* einer offenen Kommunikation. Die Technologie tritt lediglich beim „Betreten“ der Plattform in Erscheinung, die Sicherheitsfeatures sollen ansonsten im Hintergrund arbeiten und in der Kommunikation nicht zutage treten. Erst durch Sicherheit und Verlässlichkeit – so die Prämisse in den hier beschriebenen Anwendungsszenarien – ist spontane und offene Kommunikation möglich. Intelligente Zugangstechnologien ermöglichen gewissermaßen einen „unbeschwerten“ Umgang mit Kommunikations-, Transport- oder Gesundheitssystemen, indem sie die Angst vor Manipulation, Verwechslung, Missbrauch oder Fehlfunktionen minimieren.

Dabei zeigt sich allerdings auch der *ambivalente Kern der hier betrachteten Zugangs- und Überwachungstechnologien*: Zum einen schützen sie Wirtschaft und Gesellschaft vor äußeren

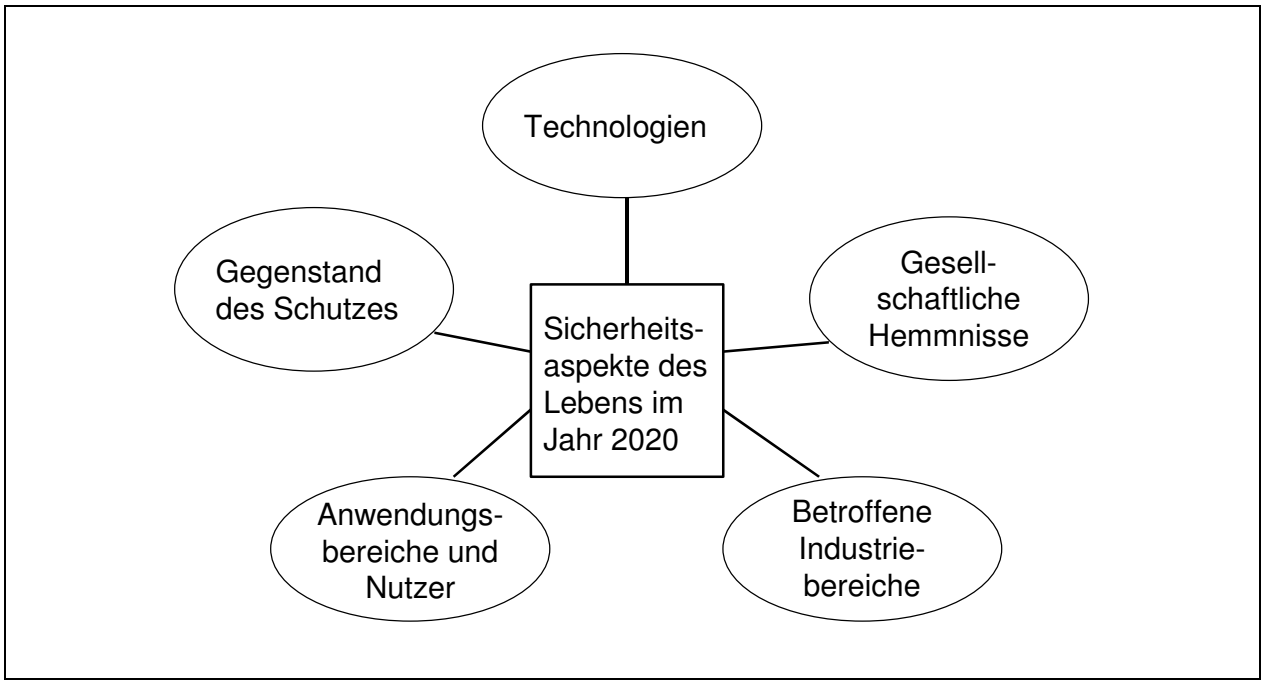
und inneren Bedrohungen, zum anderen erfordern sie die Erhebung umfangreicher Nutzerdaten und –profile, was selbst wiederum als Gefährdung der Privatsphäre oder als Verletzung der informationellen Selbstbestimmung betrachtet werden kann.

Methode und Vorgehen

Wie in der Szenariotechnik üblich, wurden zu Beginn relevante Einflussbereiche definiert, die die Entwicklung des Themas „Sicherheit im Jahr 2020“ bestimmen. Ausgangspunkt bildeten die in Tabelle 3 im vorangegangenen Abschnitt aufgeführten IT-basierten Identifikations-, Überwachungs- und Zugangstechnologien.

Entsprechend der Fragestellung wurden anschließend folgende weitere Einflussbereiche festgelegt: Gegenstand des Schutzes, Anwendungsbereiche und Nutzer, gesellschaftliche Hemmnisse und betroffene Industriebereiche (siehe Abbildung 19).

Abbildung 19: Fünf Einflussbereiche für die Szenarien 2020: „Sicherheit durch IT“



Um die Aufgaben der IT-Systeme zu spezifizieren, wurden im Einflussbereich „Gegenstand des Schutzes“ folgende Bereiche definiert:

Was soll geschützt werden?

1. Öffentliche Sicherheit (Schutz vor Anschlägen, Kriminalität, Diebstahl, und menschengemachten Umweltkatastrophen)
2. Mobilität
3. Kommunikation
4. Objekte wie z.B. Gebäude, Hardware oder Geld
5. Personen (Gesundheit, Identität, persönliche Daten)

6. Wissen (Software, Know-how, Unternehmensgeheimnisse)

Weiterhin mussten für den Einflussfaktor „Anwendungsbereich und Nutzer“ geeignete Unterpunkte gefunden werden. Im Szenarioprozess werden diese Unterpunkte in der Regel als Deskriptoren bezeichnet. Folgende Deskriptoren wurden hier festgelegt:

Anwendungsbereiche und Nutzer

1. Sicherheit im öffentlichen Raum, inkl. Sicherheit im öffentlichen Verkehr
2. Sicherheit im Auto, in Fahrzeugen allgemein, im Straßenverkehr und Sicherstellung der Mobilität
3. Flugverkehr (Passagierbereich und Flugbereich)
4. Zugang zum Unternehmen, Identitätsmanagementsysteme, Schutz von unternehmenseigenen Informationen und Objekten gegenüber Fremden, lückenlose Nachvollziehbarkeit der Aufenthaltsorte der Mitarbeiter, um sie jederzeit kontaktieren zu können.
5. Smart Secure Home (Zugang, Videoüberwachung, Notfallalarmierung)
6. Bankgeschäfte inkl. Online-Banking
7. Zugang zum Hotel, Sicheres Einkaufen
8. Medizin und Gesundheit
9. Computer und Kommunikation inkl. mobiler Kommunikation und Geräten, die erkennen, dass sie gestohlen worden sind.

Darüber hinaus sollten Aussagen möglich werden, welche Hindernisse bei der Realisierung IT-basierter Sicherheitstechnologien heute bestehen bzw. welche Hindernisse beseitigt werden müssen, damit diese im Jahr 2020 entsprechend eingesetzt werden können. Dazu wurden im Einflussbereich „Hemmnisse“ sieben Deskriptoren festgelegt:

Hemmnisse

1. Technische Reife (Einsatz in realen Situationen, Praktikabilität)
2. Akzeptanzschwierigkeiten
3. Ausfallsicherheit
4. Rechtliche Hürden
5. Datenschutz
6. Gefahr für Leib und Leben (als Akzeptanzhemmnis, beispielsweise könnte der Diebstahl einer bestimmten Netzhaut von Bedeutung werden, um sich den Zugang zu einem Bereich zu verschaffen, der über ein Iriserkennungssystem gesichert ist)
7. Täuschungs- und Ausspähfähigkeit, d.h. die Frage, ob das System gehackt werden kann.

Schließlich sollten die Industriebereiche identifizierbar sein, die speziell vom Einsatz einer bestimmten Sicherheitstechnologie betroffen sein würden. Deshalb wurden folgende Festlegungen getroffen:

Betroffene Industriebereiche

1. Softwareentwicklung
2. Hardwareproduktion
3. Datenbankenverwaltung
4. Systemintegration
5. Location based services, GPS-basierte Dienste

In einem Workshop wurde für jede der neun aufgeführten Technologien diskutiert, was diese schützen sollen (Gegenstand des Schutzes), welche Anwendungsbereiche davon betroffen sein würden (Anwendungsbereiche und Nutzer), welche Hindernisse es bei der Realisierung heute und in Zukunft voraussichtlich gibt (Hemmnisse) und schließlich, welche der aufgeführten Industrien besonders vom verstärkten Einsatz der jeweiligen Technologien betroffen sein würden. Das Ergebnis dieses Kombinationsprozesses, der in der klassischen Szenariotechnik unter der Überschrift Konsistenz- oder Cross-Impact-Analyse durchgeführt wird, zeigt Tabelle 4:

Tabelle 4: Ergebnis des Kombinationsschritts (Matrix)

Technologien	Was soll geschützt werden?	Anwendungsbereiche	Hemmnisse	Betroffene Industrien
Digitale Videoüberwachung	1, 2 (Abstandshalter, Verkehrsfluss), 4 und 5	1-7	1-5	1-4
Identitätsmanagementsysteme	4, 5, 6	4, 5, 6, 8	1, 2, 3, 7	1, 3, 4, 5
Biometrische Erkennungs- und Authentifizierungsverfahren	1-6	1 (insb. biometrische Pässe), 2-6 und 9	1-6	1-5
Chipkarten	2, 4, 5 und 6	2, 4, 5-9	2 (bei Gesundheitskarte), 5, 7	1-4
PINs und Passwörter (aktive Zugangskontrolle: man muss etwas eingeben und sich daran erinnern) sowie digitale Signatur	3, 4, 6	4-7 und 9	7	1, 2
Smart tags, RFID und elektronische Schlüssel (passive Zugangskontrolle)	1, 2 (für Fahrkarten mit RFID-Chips, Zugang zu Metro), 3, 4, 6	2, 3 (Gepäcktracking im Flugverkehr), 4 und 5, 6, 7 und 8 (RFID-Chips als Implantat), 9	1, 2, 5	1-5
Verkehrsüberwachung, Fahrzeugassistenzsysteme, Notfall, Diebstahl	1-5	1, 2	1-3, 5	1-5
Data mining zum Aufspüren verdächtiger Verhaltensmuster	1, 4	1	2, 4 und 5, 7	1, 3-5
Biochips und Biosensoren zum Monitoring der Gesundheit	5	2 (Auto erkennt, dass es seinem Fahrer schlecht geht oder einen Unfall), 8	1-3	1-5
Sensoren zum Aufspüren von Bakterien, Viren und Giftstoffen	1, 4, 5	1, 3, 8	1, 3	1-4

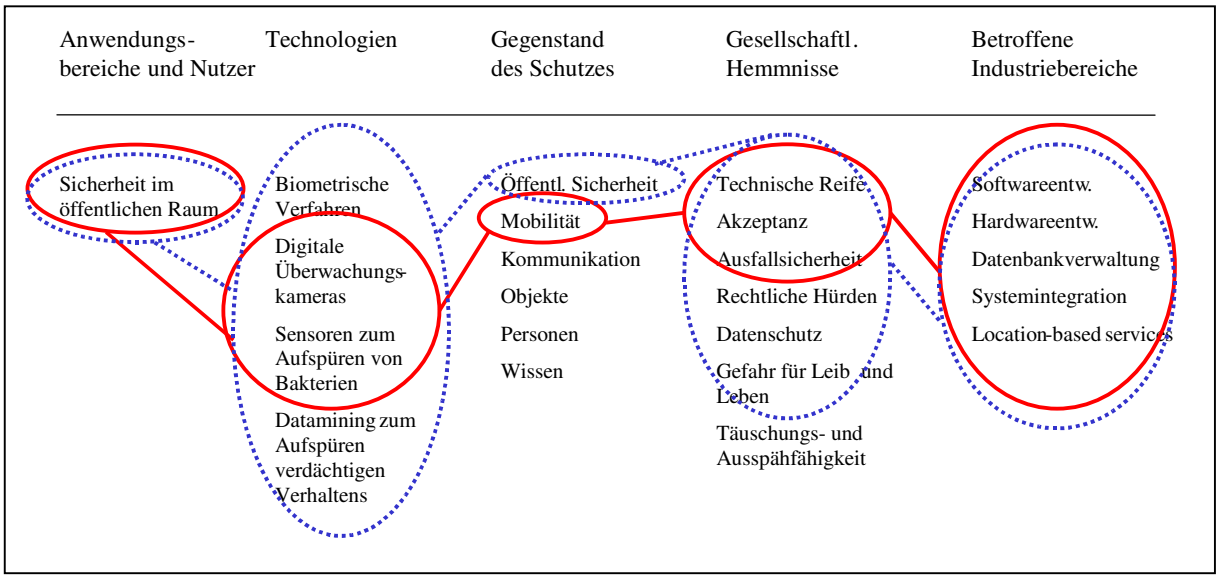
In der Zusammenschau der Ergebnisse des Kombinationsschritts zeigte sich, dass die ursprünglich neun Anwendungsbereiche aufgrund von Ähnlichkeiten zu insgesamt fünf zusammengefasst werden können. Bei diesen Anwendungsbereichen, für die im Folgenden die entsprechenden Szenarien entwickelt werden, handelt es sich um:

1. Sicherheit im öffentlichen Raum (inkl. auf Bahnhöfen)
2. Sicherheit im Auto, im öffentlichen Verkehr und im Flugverkehr (Passagierbereich und Flugbereich)
3. Sicherer Zugang zum Unternehmen und zum Smart Secure Home
4. Sicheres Online-Banking und Einkaufen im Internet (inkl. Sicherheit mobiler Geräte, die erkennen, dass sie gestohlen worden sind)
5. Sicherheit in den Bereichen Medizin und Gesundheit

Mit dem Kombinationsschritt und der Festlegung auf die fünf Anwendungsbereiche wurde eine Perspektivenverschiebung möglich: Nicht mehr die Technologien als solche stehen im Folgenden im Mittelpunkt, sondern ihre Anwendungspotenziale in den einzelnen Bereichen, ihre Barrieren bzw. kritischen Faktoren sowie die Identifizierung der jeweilig meist betroffenen Industriebereiche.

Die eigentliche Erstellung der fünf Anwendungsszenarien erfolgte auf der Basis der Kombinationstabelle (Tabelle 4), indem nun nur noch jene Technologien betrachtet wurden, die im jeweiligen Anwendungsfeld als relevant eingestuft wurden. Gleichermaßen wurde mit den Kategorien „Gegenstand des Schutzes“, „Hemmnisse“ sowie „betroffene Industriebereiche“ verfahren. Da es meist mehr als einen plausiblen Kombinationsstrang gibt, wurden die Verbindungen in unterschiedlichen Graustufen dargestellt (siehe Abbildung 20).

Abbildung 20: Identifikation von plausiblen Kombinationssträngen am Beispiel des Anwendungsbereichs „Sicherheit im öffentlichen Raum“



Das Verfahren bietet den Vorteil, dass es umgekehrt auch möglich ist, zu zeigen, in welchen Anwendungsbereichen die verschiedenen Technologien Verwendung finden. Dies ist beispielhaft in Tabelle 5 dargestellt.

Tabelle 5: Kombinationsmöglichkeiten aus der Perspektive der Technologien

	Ausprägungen					
	1	2	3	4	5	6
Anwendungsbereiche und Nutzer	Sicherheit im öffentlichen Raum	Auto, Fahrzeuge, Straßenverkehr und Mobilität, Flugverkehr (Passagierbereich und Flugbereich)	Zugang zum Unternehmen, (Identitätsmanagementsysteme, um knowledge-sharing und Kooperation zu verbessern) Schutz eigener Informationen und Objekte gegenüber Fremden, Gebäudetechnik (Fluchtwegoptimierung, lückenlose Nachvollziehbarkeit der Aufenthaltsorte der Mitarbeiter, um sie jederzeit kontaktieren zu können) // Smart secure Home (Zugang, Videoüberwachung, Notfallalarmierung)	Bankgeschäfte inkl. Online-Banking // Zugang zum Hotel, Einkaufen	Medizin und Gesundheit	Computer/Kommunikation inkl. mobiler Kommunikation und Geräten, die erkennen, dass sie geklaut worden sind
Technologien	Biometrische Erkennungs- und Authentifizierungsverfahren	Digitale Videoüberwachung	Chipkarten	RFID und eletronische Schlüssel (passive Zugangskontrolle)	PINs und Passwörter (aktive Zugangskontrolle, man muss etwas eingeben und sich daran erinnern)	Digitale Signaturen
Gegenstand des Schutzes	Öffentliche Sicherheit (Schutz vor Anschlägen, Kriminalität, Diebstahl, menschengemachte Umweltkatastrophen)	Mobilität	Kommunikation	Objekte wie z.B Gebäude, Hardware, Geld	Personen (Gesundheit, Identität, perönliche Daten)	Wissen (Software, Knowhow, Unternehmensgeheimnisse)
Gesellschaftliche Hemmnisse	Technische Reife (Einsatz in realen Situationen, Praktibilität)	Akzeptanzschwierigkeiten	Ausfallsicherheit	Rechtliche Hürden	Datenschutz	Gefahr für Leib und Leben
Betroffene Industrien	Softwareentwicklung	Hardwareproduktion	Datenbankenverwaltung	Systemintegration	Location based services, GPS-basierte Dienste	

Die Tabelle zeigt am Beispiel der Technologie „Smart Tags, RFID und elektronische Schlüssel“, welche Kombinationen sich mit den anderen Kategorien ergeben. Dabei basiert die Tabelle auf denselben Daten wie Abbildung 19, sie stellt die Ergebnisse des Kombinationsschritts (siehe Tabelle 4) aber in anderer Reihung dar.

Die fünf Anwendungsszenarien

Die fünf Anwendungsszenarien entstanden als *Ergebnis eines Kombinationsprozesses*, der sich an die klassische Szenariomethode anlehnt und bei dem für jeden der fünf festgelegten Bereiche spezifische „Ring-Kombinationen“ erstellt wurden. Die Ringe in den jeweiligen Abbildungen bezeichnen mögliche und plausible Kombinationsbündel, die sich in der Zusammenschau zu Kombinationssträngen vereinigen. Im zweiten Schritt wurden die so erzielten Ergebnisse anhand von Beispielen und Fundstellen aus der Literatur (Fallstudien, Szenarien, Technologie-Roadmaps usw.) illustriert. Das Ergebnis dieses Prozesses wird im Folgenden dargestellt.

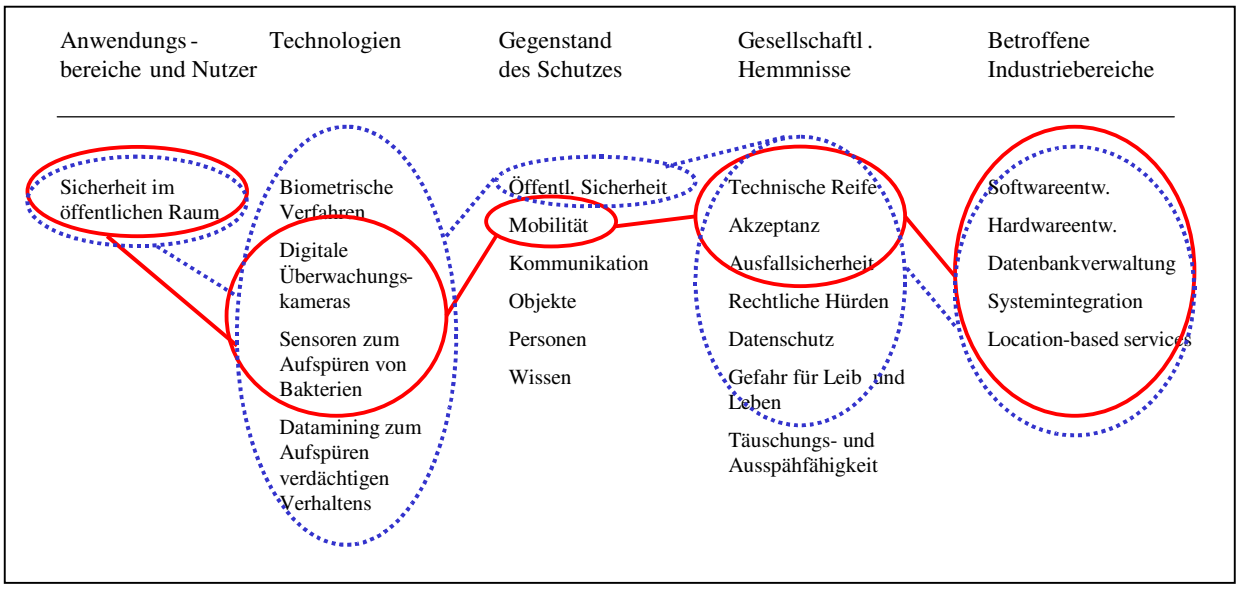
Die Leitfrage bei der Darstellung der Szenarien lautet: Was hat die IT dazu beigetragen, dass dieser Bereich (öffentliche Sicherheit, Verkehr, Unternehmen und Home, Online-Banking und Gesundheit) im Jahr 2020 sicherer geworden ist? Dabei stehen Zugangs-, Identifikations- und Überwachungstechnologien im Vordergrund, die in den spezifischen Zusammenhang des Anwendungsgebietes gebracht werden.

Szenario 1: Sicherheit im öffentlichen Raum

Das erste Szenario zeichnet sich durch Kombinationsmöglichkeiten aus, die in Abbildung 21

dargestellt sind.

Abbildung 21: Kombinationen im Szenario: Sicherheit im öffentlichen Raum



Die wesentlichen Aussagen dieses Szenarios lassen sich folgendermaßen zusammenfassen:

2020 werden wir...

- ➔ … vor Bahnfahrten unser Handgepäck in einer Sicherheitsschleuse durchleuchten lassen und nur mit RFID-Ausweis Zutritt erhalten.
- ➔ … von Tausenden von Videokameras beobachtet werden, die auf allen öffentlichen Plätzen installiert sind. Die Bilddaten werden aber nicht von Menschen ausgewertet, sondern von Computern. „Intelligente“ Erkennungssoftware wird dafür sorgen, dass nur verdächtige Personen und Objekte (z.B. herrenlose Gepäckstücke) registriert werden. Das System löst dann automatisch Alarm aus.
- ➔ … uns sicherer fühlen, weil Biosensoren weit verbreitet sind, die gefährliche biologische und chemische Stoffe aufspüren können und rechtzeitig Alarm auslösen.

Wichtigste Barrieren sind...

- ➔ … technische Reife: Zuverlässigkeit, Erkennungsraten, Sensitivität der Kameras, Vernetzung heterogener Datenbestände, Analyse großer Datenbestände.

Kritische Faktoren sind...

- ➔ … gesellschaftliche Akzeptanz: Straftaten gehen zurück bei Überwachung, aber: Wie kann Datenschutz überzeugend sichergestellt werden?

Einen facettenreichen Einblick in die Potenziale der Informationstechnik zur Erhöhung der öffentlichen Sicherheit und insbesondere der Sicherheit vor terroristischen Anschlägen erlaubt der Patriot Act der Bush-Administration. Im Patriot Act von 2003 war ein Programm zur totalen Überwachung vorgesehen, ein Gesetz, das unter dem Namen „Terrorist Information

Awareness“ (TIA) bekannt wurde. TIA war die Utopie der Informationssammler. Das Information Awareness Office erhielt die Aufgabe, so viele Daten wie irgend möglich zentral zusammenzutragen: Internet-Aktivitäten, Käufe mit Kreditkarten, Flugbuchungen und Angaben über gemietete Autos und Verschreibungen von Medikamenten, Schulzeugnisse, Rechnungen der Stadtwerke, Steuerbescheide usw. (vgl. Steinmüller 2006, S. 247). Geplant war, dass die amerikanische Wehrforschungsbehörde DARPA das TIA mit 53 Millionen Dollar finanziert. Diese Gelder sollten vor allem in die Entwicklung von Informationstechnik fließen. Die Utopie der Initiatoren der TIA fasst Steinmüller folgendermaßen zusammen: „Eine Transkriptionssoftware verwandelt Sprache in Text, wodurch sich endlich Telefongespräche automatisch auswerten lassen. Selbstverständlich werden auch fremdsprachliche Gespräche und Texte übersetzt, und die Software fasst dazu noch den Inhalt zusammen. Eine fortgeschrittene Gesichtserkennung funktioniert auch im Freien und bei schlechter Beleuchtung. Menschen werden durch Radar aus der Distanz aufgespürt und anhand ihrer Bewegungsmuster identifiziert. All diese Pentabyte von Daten laufen zusammen und werden in neuartigen Datenbanksystemen gespeichert und analysiert. Bei einer Krise ermöglicht ein komplexes System, Entscheidungen partiell automatisch zu fällen. Individuelles Verhalten und soziale Netzwerke werden ebenfalls analysiert und auf dieser Grundlage terroristische Anschläge automatisch vorhergesagt. Und neue kontextbezogene Visualisierungsmöglichkeiten gestatten es auch Nichtexperten, die Zusammenhänge schneller zu verstehen.“ (Steinmüller 2006, S. 248). Soweit die Utopien der Entwickler und IT-Sicherheitsexperten. Tatsächlich erregte die Einrichtung einer Terrorist Information Office mit derartig weit reichenden Zielsetzungen massiven Widerstand in der amerikanischen Bevölkerung, insbesondere bei Bürgerrechtlern. Mitte 2003 strich der amerikanische Senat in aller Stille das TIA aus dem Budget des Pentagons: „Damit wurde den Orwell’schen Visionen zwar die Spitze abgeschnitten, ein Großteil der Forschungen läuft jedoch weiter“, so Steinmüller (2006, S. 248).

Einzelne Teile der beschriebenen Utopie der Entwickler stellen bei genauerer Betrachtung der ermittelten Kombinationsbündel im Szenario tatsächlich eine Option zur Erhöhung der Sicherheit im öffentlichen Bereich im Jahr 2020 dar: Zum einen kann davon ausgegangen werden, dass im Jahr 2020 die Videoüberwachung in Bahnhöfen, Zügen, Flughäfen, in der Stadt, im Einkaufszentrum, im Stadion usw. sehr dicht sein wird und sich Deutschland an die heutige Situation in Großbritannien angenähert haben wird. Dabei werden die Videobilder allerdings nicht von Menschen ausgewertet, sondern von Computern. Es wird intelligente Erkennungssoftware geben, Non-Motion-Capturing-Verfahren, die herrenlose Gepäckstücke erkennen und auch Biosensoren werden weit verbreitet sein, womit sich gefährliche Stoffe wie z.B. Sprengstoffe aufspüren lassen. Ebenso wird dann die automatische Gesichtserkennung auch bei schlechten Lichtverhältnissen funktionieren, weil die Entwicklung optischer Technologien weiter fortgeschritten sein wird. Die Menschen werden für eine höhere Sicherheit weitgehend akzeptieren, dass sie an öffentlichen Plätzen unbeobachtet überwacht werden und dass ihre Daten mit den Einträgen und Profilen von Straftätern oder Verdächtigen abgeglichen werden. Zum anderen wird es immer mehr Sicherheitsschleusen geben, wie sie vom Flughafen bekannt sind. Auch beim Eingang zur U-Bahn und an anderen neuralgischen Punkten wird es Sprengstoffdetektoren und Personenkontrollen geben. An diesen Kontrollpunkten werden Personen schneller

abgefertigt, die einen speziellen RFID-Ausweis besitzen. Weiterhin wird es im Jahr 2020 üblich sein, dass die Lkw-Mautstationen auf Autobahnen auch zur Überwachung von Mobilitätsmustern und zur Fahndung genutzt werden.

Ein Grund für die weitgehende Akzeptanz der Bevölkerung für die Überwachungsmaßnahmen ist, dass die Überwachungsdaten nach einem halben Jahr wieder gelöscht werden. Darüber hinaus wird die Gesetzgebung darauf achten, dass die Daten nur zur Aufklärung von Verbrechen und zur Verfolgung von Straftaten verwendet werden. Das Vertrauen der Bürger in die Sorgfalt des Staates im Umgang mit diesen Daten ist für dieses Szenario eine wesentliche Voraussetzung. Diese Erwartung wird von empirischen Daten aus der Gegenwart unterstützt: Nach einer Umfrage von Eurostat aus dem Jahr 2003 glauben 55 Prozent der Deutschen, dass Behörden verantwortungsvoll mit ihren Daten umgehen, nur 39 Prozent trauten dagegen ihren Kreditkarten-Unternehmen (Cziesche et al. 2007, S. 65).

Insbesondere nach einer Reihe von terroristischen Anschlägen in Deutschland wird die Bevölkerung bereit sein, umfangreiche Sicherheitsmaßnahmen mitzutragen, auch wenn nicht immer gewährleistet scheint, dass die eingesetzten Technologien effizient und wirklich in der Lage sind, Anschläge gänzlich zu verhindern. „Der Bürger hat ein Recht darauf, morgens zur Arbeit zu fahren, ohne erwarten zu müssen, in die Luft gesprengt zu werden“, so der berühmte Ausspruch von Charles Clarke, dem ehemaligen britischen Innenminister und Initiator des EU-Beschlusses zur Vorratsdatenhaltung (zitiert in Cziesche et al. 2007, S. 69). Dieser Ausspruch könnte als Leitmotiv für dieses Szenario dienen. Für den Schutz gegen Terroristen akzeptieren die Deutschen bereits heute Kameras allerorten, elektronische Chips im Reisepass und die weit reichende Überwachung ihrer Telekommunikation. Wer nichts zu verbergen habe, müsse auch nichts befürchten, so das Argument der Kontrolleure (vgl. Cziesche et al. 2007, S. 64f).

Auch bei der Bekämpfung von Straßenkriminalität hat man sich an die allgegenwärtige Überwachung gewöhnt. Sie verschafft ein Gefühl von Sicherheit: Am Münchner Bahnhof etwa sank nach dem Einbau von Kameras die Kriminalitätsrate um die Hälfte. In Leipzig, wo die Innenstadt überwacht wird, gingen die Straftaten innerhalb weniger Jahre von 542 auf 70 zurück (Cziesche et al. 2007, S. 68).

Prinzipielle Voraussetzung für öffentliche Sicherheit ist es, Gefährdungsquellen frühzeitig zu entdecken und zu analysieren. Überwachungs- und Identifikationstechnologien sind hierfür der Schlüssel. Die Verfahren reichen von der weltweiten und langfristigen Überwachung kritischer Gebiete mit satellitengestützter Fernerkundung bis zur Kontrolle an Grenzübergängen oder des Zutritts zu Räumen wie Bankgebäuden und Abfertigungshallen in Flughäfen. Ein Kernfeld ist dabei wie bereits erwähnt die Detektion und Überwachung von Sprengstoffen, chemischen, biologischen und nuklearen Agenzien (vgl. Horn 2007, S. 37). Hierfür werden im Jahr 2020 spezielle Sensoren eingesetzt. Bei Sensoren handelt es sich um so genannte „sicherheitsfördernde Technologien“, d.h. Technologien, die nicht mit dem Schwerpunkt auf Sicherheit entwickelt wurden, aber dennoch wesentlich zum Aufbau eines Sicherheitssystems beitragen können. Hierunter fallen z.B. Sensormeldesysteme zur Überwachung physischer Zustände – z.B.

multifunktionale Radar-Sensoren und faseroptische Sensoren zur Messung physikalischer Größen oder zur Erkennung gefährlicher Substanzen. Ein Beispiel ist die Überprüfung von Transportbehältern. Verteilte Sensoren können beim Be- und Entladen Daten über den aktuellen Zustand innerhalb des Containers liefern. So wurden Sensoren entwickelt, mit deren Hilfe sich eine automatische Vor-Ort-Analyse gefährlicher chemischer oder biologischer Substanzen in Luft und Flüssigkeiten schnell durchführen lässt. So wie heute die Luftqualität in Innenstädten regelmäßig überprüft wird, könnten künftig so genannte weiche Ziele permanent auf Spuren von atomaren, biologischen und chemischen (ABC)-Waffen hin überwacht werden. Ein oder zwei größere Anschläge könnten genügen, damit in den Innenstädten neben Überwachungskameras auch B- und C-Alarmmelder angebracht werden (Steinmüller 2006, S. 253). Auch mobile Ad-hoc-Netze oder selbstoptimierende Kommunikationsnetze sind sicherheitsfördernde Technologien. Denn sie können helfen, die Kommunikation trotz teilweise ausgefallener Infrastrukturen aufrechtzuerhalten (vgl. Trage 2006, S. 33).

Interessante Hinweise auf die Wahrscheinlichkeit des Eintretens der dargestellten Entwicklungen gibt der Delphi-Bericht „Wie werden wir Informations- und Kommunikationstechniken im Jahre 2020 nutzen?“, der ebenfalls im Rahmen des Projekts FAZIT-Forschung erstellt wurde (von Oertzen, Cuhls, Kimpeler 2006). Dort wurden zum Thema „Wie viel Sicherheit wird IKT im Jahr 2020 bieten?“ folgende Aussagen getroffen:

Für *wahrscheinlich* bis zum Jahr 2020 halten die Befragten im Durchschnitt die folgenden Thesen:

Biometrische Zugangskontrollen zu öffentlichen Gebäuden und Arbeitsstätten werden allgemein akzeptiert.

Neben der Kriminalitätsvermeidung und -bekämpfung dient die *ständige Überwachung* des öffentlichen Raumes auch dazu, Ordnungswidrigkeiten konsequent zu verfolgen.

Gewaltdelikte sind verbreitet, mit denen sich Kriminelle Zugang zu biometrisch gesicherten Bereichen verschaffen wollen.

Für *möglich* bis zum Jahr 2020 halten die Befragten im Durchschnitt die folgenden Thesen:

Das *Informationsrecht* gegenüber staatlichen Stellen (Akteneinsicht etc.) ist deutlich verringert worden, um die öffentliche Sicherheit zu erhöhen.

Zur Verbrechensbekämpfung ist eine weit reichende *Erhebung von privaten Daten* und deren automatisierte Auswertung durch staatliche Instanzen allgemein erwünscht.

Für *unwahrscheinlich* bis zum Jahr 2020 halten die Befragten im Durchschnitt die folgenden Thesen:

Das Recht auf *informationelle Selbstbestimmung* ist weiterentwickelt worden und gibt dem Einzelnen weit reichende Möglichkeiten zu entscheiden, wer welche Daten von ihm erhält und wo er lieber anonym bleiben möchte.

Die automatische Erfassung aller *persönlichen Bewegungen* wird allgemein akzeptiert.

Quelle: von Oertzen, Cuhls, Kimpeler 2006, S. 84ff.

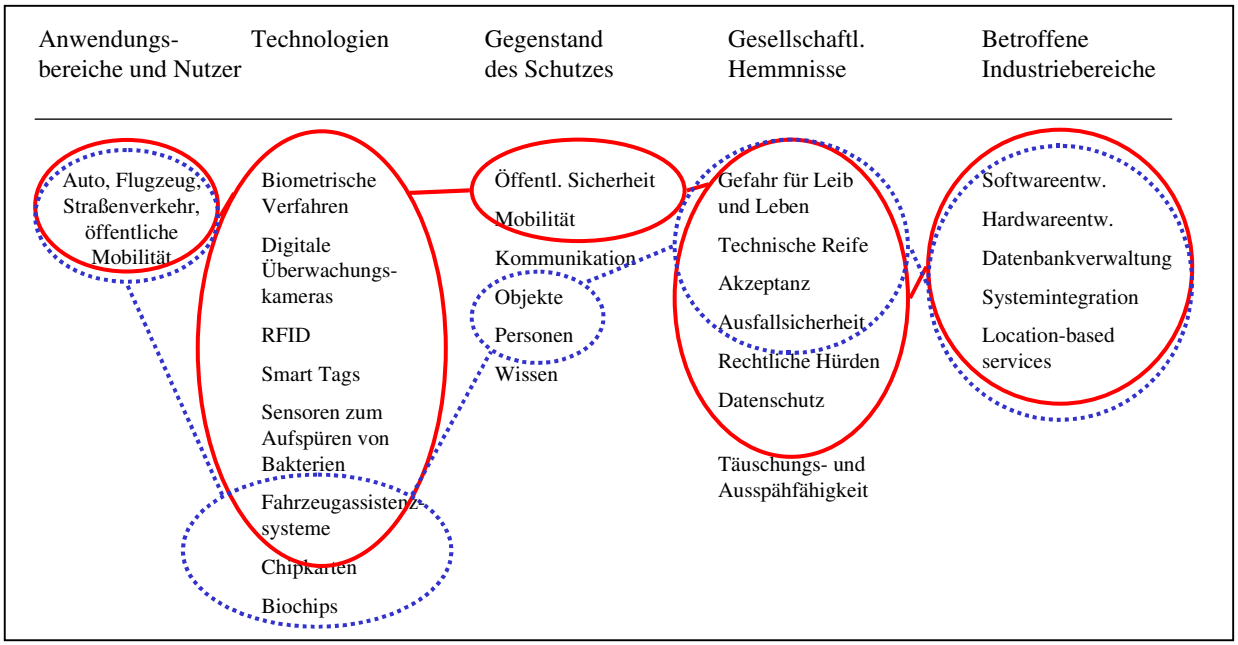
Betrachtet man die künftigen Entwicklungs- und Einsatzpotenziale von IT zur Erhöhung der öffentlichen Sicherheit, so zeigen sich zwei generelle Mechanismen: Zum einen machen sich Kriminelle neue Technologien genauso zu eigen wie staatliche oder private Akteure, die ihre Bestände und Systeme gegen Ausspähung, Manipulation oder Zerstörung schützen wollen. Früher oder später werden auch jene Sicherheitseinrichtungen überwunden, die bis dahin als uneinnehmbar gegolten hatten. Das bekannte Katz-und-Maus-Spiel setzt sich mit jeder neuen Technologiewelle fort, woraus sich generelle Effektivitätsbedenken ergeben.

Zum anderen hängt die Akzeptanz von Maßnahmen zum Schutz der öffentlichen Sphäre von der jeweils aktuellen Bedrohungslage ab: Werden sich in Deutschland terroristische Anschläge ereignen oder kriminelle Gefährdungen stärker ins Bewusstsein der Bevölkerung treten, sind Maßnahmen zur Überwachung öffentlicher Räume, die Erhebung und Speicherung von Mobilitätsmustern oder Kommunikationsdaten sowie verschärfte Kontrollen aller Art eher akzeptabel. Wird die Bedrohungssituation dagegen allgemein als weniger gravierend betrachtet, werden neue Technologien zur Identifizierung und Überwachung kaum Akzeptanz finden, bzw. von Teilen der Bevölkerung bewusst abgelehnt und sogar bekämpft werden.

Szenario 2: Sicherheit im Auto, im öffentlichen Verkehr und im Flugverkehr

Das zweite Szenario zeichnet sich durch Kombinationsmöglichkeiten aus, die in Abbildung 22 dargestellt sind.

Abbildung 22: Kombinationen im Szenario: Sicherheit im Auto, im öffentlichen Verkehr und im Flugverkehr



Die wesentlichen Aussagen dieses Szenarios lassen sich folgendermaßen zusammenfassen:

2020 werden wir...

- ➔ … mehr Sicherheit im Flugverkehr durch „intelligente“ Videoüberwachung von Passagieren, Gepäck und Flughafenbereich sowie durch „Digital Graffiti“ auf Rollbahnen haben.
- ➔ … uns auf Bahnhöfen sicherer fühlen (Zugangskontrolle), weil hunderte Videokameras verdächtige Verhaltensweisen und Gefahrenquellen autonom aufspüren können.
- ➔ … sicherer Auto fahren, weil Fahrerassistenzsysteme im breiten Einsatz sind (automatische Abstandshalter, Spurhalte- und Alarmsysteme, Einschlafwarner usw.).

Wichtigste Barrieren sind...

- ➔ … im Flugverkehr: Standardisierung, Synchronisierung von internationalen Datenbeständen, Fehlalarme.
- ➔ … beim Auto: Kontrolle wird an IT-Systeme abgegeben, Koordinierung der Übergangszeit, bis alle Autos Assistenzsysteme eingebaut haben.

Kritische Faktoren sind...

- ➔ … die Sicherstellung des Datenschutzes und die Überzeugung der Passagiere, dass Maßnahmen richtig und notwendig sind.
- ➔ … Auto: die Verlässlichkeit der Systeme und die Klärung von Haftungsfragen.

In diesem Szenario wird ein Sicherheitsbegriff verwendet, der weiter gefasst ist als im Szenario „Öffentliche Sicherheit“. In diesem Szenario steht die sichere, optimierte und hoch verfügbare Mobilität im Mittelpunkt, die z.B. durch Fahrerassistenzsysteme oder Verkehrsleitsysteme, durch „intelligente“ Zugangskontrollen im öffentlichen Nahverkehr oder durch digitale Sicherheitssysteme auf Flughäfen gekennzeichnet ist.

Verkehrsmanagementsysteme und Navigationshilfen werden bereits heute zur Verbesserung der Sicherheit im Autoverkehr eingesetzt. Künftig werden Technologien zur Fahrerassistenz von so genannten Head-up Displays ergänzt, die die jeweils erforderlichen Informationen automatisch auf die Frontscheibe projizieren. Folgende Assistenzsysteme werden im Jahr 2020 den Autofahrer wie selbstverständlich begleiten: Spurwechselwarnung, intelligente Geschwindigkeitsanpassung, Verkehrszeichenerkennung, Kollisionswarnung, Toter-Winkel-Erkennung mit Kameras statt Rückspiegeln und Ermüdungswarnung (vgl. Aschenbrenner 2005).

Dabei sind es insbesondere die neuartigen Sensoren, die das Auto sicherer machen werden: Bereits heute stecken in modernen Autos ca. einhundert Sensoren bzw. Messfühler. In Zukunft könnten noch mehr und leistungsfähigere sowie vernetzte Sensoren das Autofahren sicherer machen, beispielsweise durch Sensoren im Reifen. Diese könnten nicht nur bei zu wenig Reifendruck Alarm schlagen oder Defekte im Reifen selbständig entdecken, sondern in Zukunft auch die Profiltiefe erkennen und den Fahrer entsprechend informieren (Gerl 2004). Im Autoinnenraum (oder in klimatisierten Gebäuden) könnten Sensoren für Kohlendioxid (CO2) auf

schlechte Luftqualität aufmerksam machen und so Übermüdungen aufgrund fehlenden Sauerstoffs verhindern.

Neben den Sensoren sind es vor allem moderne Kameras, die die Sicherheit beim Autofahren in der Zukunft erhöhen werden. Als Bestandteil von Fahrerassistenzsystemen werden heute kamerabasierte Spurhalte- und Alarmsysteme, Einschlafwarner, Systeme zur gezielten Auslösung von Airbags sowie Lösungen zur Erkennung von Fußgängern entwickelt. Künftig werden Systeme der automatischen Bildverarbeitung in die Fahrerassistenzsysteme im Auto integriert. Treiber dieser Entwicklung ist die Fähigkeit der Systeme, die Bilddaten auch zu interpretieren und Informationen von einer großen Anzahl von Sensoren sinnvoll zusammenzufügen (Pease 2006, S. 83). Hier werden Radar-, Infrarot-, Ultraschall- und drahtlose Kommunikationssysteme zusätzliche Sensorinformationen liefern, um in der Nähe befindliche Fahrzeuge zu erkennen und mit ihnen in Verbindung zu treten bzw. um diese auf Abstand zu halten. Auf diese Weise können Unfälle vermieden werden, die auf tote Winkel, plötzliche Bremsmanöver und schlechte Sichtverhältnisse zurückzuführen sind. Irgendwann werden die Lösungen dann als komplette Pakete angeboten, in denen die Daten aller Sensoren logisch zusammengeführt werden und die die Grundlage für eine autonome Steuerung des Autos bilden (vgl. Pease 2006, S. 85).

Eine autonome Steuerung beinhaltet allerdings, dass die Kontrolle über das Fahrzeug vom Fahrer an die IT übergeben wird – ein Vorgang, der versicherungstechnisch nicht unproblematisch ist. Eine andere Barriere stellt die Koordinierung der Übergangszeit da, bis in alle Autos Assistenzsysteme eingebaut sind. Systeme zur Steuerung von Verkehrsströmen sind darauf angewiesen, dass alle am Straßenverkehr teilnehmenden Fahrzeuge erfasst werden und nicht nur z.B. Fahrzeuge der Oberklasse, die als erste mit den neuen Systemen ausgestattet werden.

Sicherheit vor Diebstahl und Ausfallsicherheit durch die Verwendung von Originalersatzteilen sind weitere Einsatzbereiche IT-gestützter Sicherheitstechnologien im Auto. Im Szenario des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sind beispielsweise Radio Frequency Identification (RFID)-Etiketten, die sich nicht mehr entfernen lassen, bei vielen Gütern zum integralen Bestandteil des Produkts geworden: „RFID-Tags werden sukzessive weiteren Einzug in die alltäglichen Gegenstände des Lebens halten. Vor allem hochwertige und fälschungsgefährdete Produkte werden zunehmend mit einem passiven RFID-Transponder ausgestattet sein. Hierzu können beispielsweise Produkte der pharmazeutischen Industrie, der Automobilindustrie oder der Textil- und Modebranche zählen. (...) Die Kosten für den Einsatz der RFID-Technologie werden voraussichtlich moderat sinken, die Standardisierung wird in Teilbereichen weiter voranschreiten“, so das BSI in seiner RFID-Studie aus dem Jahr 2005 (S. 96).

Das Auto wird als Beispiel für Anwendungsmöglichkeiten für RFID-Etiketten angeführt. Die elektronischen Systeme der Autos der Zukunft werden Austauschteile nur noch bei Vorhandensein eines auf dem RFID-Tag gespeicherten Autorisierungsschlüssels akzeptieren. Dadurch werden billige Plagiate von Ersatzteilen vom Markt verdrängt und die Sicherheit erheblich gesteigert (vgl. BSI 2005, S. 97).

Für die Autoindustrie könnte der durchgehende Einsatz von RFID-Tags allerdings auch negative Auswirkung haben: „Die meisten neu hergestellten Autos enthalten ein RFID-System, das die Originalität und das Alter von Ersatz- und Austauschteilen (z. B. Reifen) automatisch überwacht. Diese sind mit RFID-Tags und teilweise auch mit Sensoren ausgestattet. In Vertragswerkstätten werden Teile, die eine vom Hersteller vorgegebene Maximallebensdauer erreicht haben oder deren Nutzungslizenz erloschen ist, erkannt und gewechselt. Es können nur Austauschteile von lizenzierten Herstellern eingebaut werden. Der Bordcomputer prüft und akzeptiert diese anhand ihrer verschlüsselten ID-Codes. Ohne das Vorhandensein einer noch gültigen ID verweigert das Fahrzeug die Funktion“ (BSI 2005, S. 97). Die Hersteller werden diese Vorgehensweise mit Sicherheitsargumenten legitimieren, die Kunden können diese jedoch nicht im Detail nachprüfen und sind gezwungen, dem Hersteller blind zu vertrauen. „Als Konsequenz werden RFID-Tags aus Unfallfahrzeugen, deren Zeitlimit noch nicht abgelaufen ist, auf dem Schwarzmarkt gehandelt,“ so die BSI-Einschätzung.

Im öffentlichen Verkehr wird die IT bis zum Jahr 2020 dazu beigetragen haben, dass sich die Menschen auf Bahnhöfen, in U-Bahnen, Zügen und Bussen sicherer fühlen, weil viele Videokameras verdächtige Verhaltensweisen und Gefahrenquellen autonom aufspüren können. Diese Entwicklung wurde ausführlich bereits im Szenario für die öffentliche Sicherheit beschrieben. Aber auch an anderer Stelle trägt IT dazu bei, den öffentlichen Verkehr sicherer zu machen, nämlich bei Leit- und Sicherungssystemen, wie sie zurzeit aufgebaut werden. So kontrolliert beispielsweise das europäische Zugsicherungssystem „Trainguard“ Standort, Geschwindigkeit und Richtung jedes einzelnen Zuges und bietet damit ein Höchstmaß an Sicherheit und zugleich kürzere Taktzeiten, weil die Züge in kürzeren Abständen fahren können (vgl. Hassenmüller 2007, S. 102).

Besondere Impulse für die Erhöhung der Sicherheit sowohl im öffentlichen Verkehr als auch im Flugverkehr sind von der Weiterentwicklung von Kamerasystemen zu erwarten, die selbständig auffällige Ereignisse erkennen können. Künftig werden Kameras selbständig herrenlose Gepäckstücke in Flughäfen entdecken oder Menschen, die in U-Bahnhöfen gefährlich nahe an die Gleise kommen oder Autos, die in Tunnel in die falsche Richtung fahren. Hatten derartige Überwachungssysteme früher häufig falschen Alarm ausgelöst, so wird heute oft bereits eine Erkennungsrate von über 95 Prozent erreicht (vgl. Pease 2006, S. 83). Während sich frühere Geräte durch Reflexionen, Verdeckungen oder starke Kontraste irritieren ließen, können neue Systeme mit intelligenten Algorithmen die Bewegung von Objekten kontinuierlich verfolgen. So kann sich das Sicherheitspersonal ganz auf die Entscheidung konzentrieren, ob die Ereignisse sofortige Maßnahmen erfordern oder nicht. Dies ist wichtig, weil die Zahl der Kameras in Zukunft stark zunehmen wird.

Die Kameras werden hierfür mit eigener Rechen- und Speicherkapazität bestückt, die Entscheidungen darüber ermöglicht, welche optischen Informationen relevant sind und welche nicht. Unwichtige Daten werden herausgefiltert und nur die relevanten Informationen an die Zentrale übertragen. Damit werden keine unnötigen Datenberge produziert. Außerdem können Zehntausende kleiner, drahtloser Kameras vernetzt werden, die dann ununterbrochen Ausschau halten

nach Anzeichen von Gefahren, jede Veränderung registrieren und nur noch eine Art von Notizen austauschen und vergleichen. Dadurch wird es möglich, Tausende von Ereignissen simultan zu beobachten. Beispielsweise können die Kameras dann charakteristische Eigenschaften von Objekten erkennen und sie untereinander austauschen, um diese Objekte sozusagen von Kamera zu Kamera weiterzureichen und ihre Bewegung zu verfolgen (Pease 2006, S. 84).

Auch die Überwachungskameras, die ein Eindringen in das Flughafengelände verhindern, werden in Zukunft die Funktionen der automatischen Bewegungserkennung und -analyse und der Objektverfolgung beherrschen. Hierfür sind jedoch technische Weiterentwicklungen bei der intelligenten Bilderkennung und -verarbeitung notwendig.

Barrieren sind hier neben der technischen Reife Standardisierungsfragen sowie die Synchronisierung von internationalen Datenbeständen. Außerdem stellt sich erneut die Frage, welche Widerstände es in der Bevölkerung gegen derart umfangreiche Überwachungsmaßnahmen geben wird. Die Überzeugung von der Notwendigkeit der allgegenwärtigen automatisierten Beobachtung sowie die gesetzliche Sicherstellung des Datenschutzes sind hier die entscheidenden Faktoren.

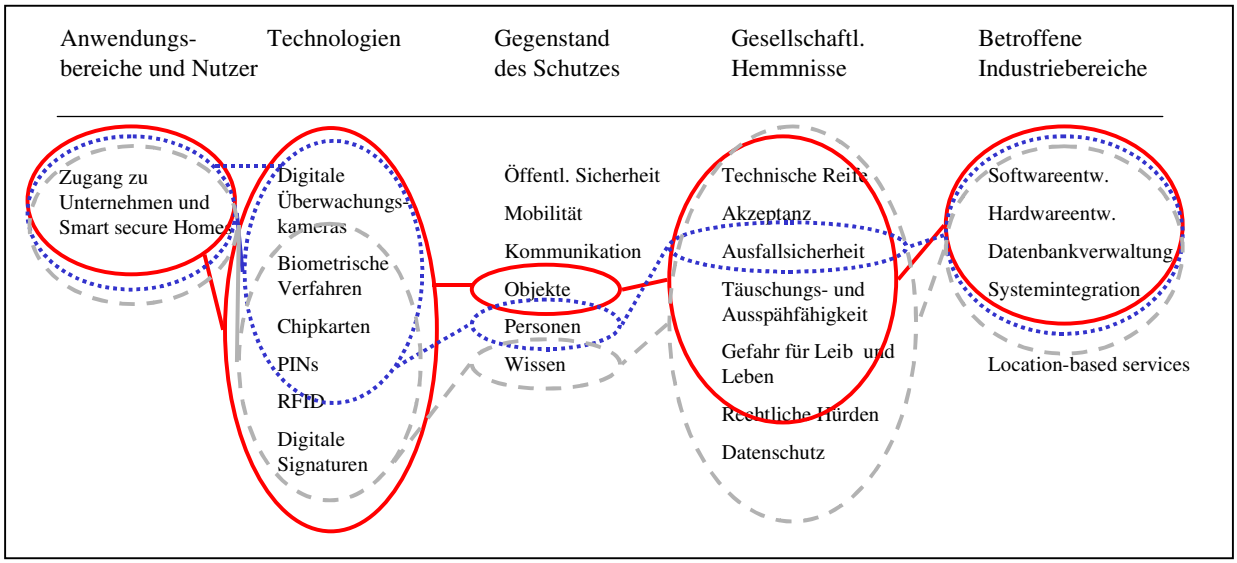
Eine weitere sicherheitsrelevante IT-Lösung für den Flugverkehr findet sich auf dem Rollfeld: „Digital Graffiti“ wird in Zukunft verhindern, dass zwei Flugzeuge versehentlich ein und dasselbe Rollfeld benutzen (vgl. Hassenmüller 2007, S. 101). Digitale Graffiti sind gewissermaßen elektronische Post-its, die das empfangende Gerät immer dann aktivieren, wenn ein bestimmter Ort betreten bzw. befahren wird.

Dabei ist diese Anwendung nicht auf den Flughafenbereich beschränkt. Mit dem Handy kann man überall Nachrichten hinterlassen, auf die dann Personen hingewiesen werden, die an diesen Ort kommen. Anders als bei der SMS klingelt das Telefon des Empfängers nur dort, wo es sinnvoll ist, nämlich in der Nähe der platzierten Botschaft. Mit Hilfe einer verfeinerten GPS-Positionsbestimmung sendet das Handy eine geographisch abgestempelte Nachricht mit einer Ortsgenauigkeit von bis zu 30 Zentimetern an einen Server. Digitale Graffitis könnten somit auch als Wegweiser oder elektronische Führer für Touristen oder Museumsbesucher eingesetzt werden. Dann kann ein Anwender sein Telefon fragen, wo die Renoir-Gemälde hängen und sich von dem Gerät den Weg weisen lassen (vgl. Pease 2004, S. 40).

Szenario 3: Sicherer Zugang zu Unternehmen und zum Smart Secure Home

Das dritte Szenario zeichnet sich durch Kombinationsmöglichkeiten aus, die in Abbildung 23 dargestellt sind.

Abbildung 23: Kombinationen im Szenario: Sicherer Zugang zu Unternehmen und zum Smart Secure Home



2020 werden wir...

- ➔ … keine Schlüssel mehr bei uns tragen, um Einlass ins Unternehmen oder zum Smart Home zu erhalten, sondern uns mit Chipkarten oder RFID-Chips ausweisen, auf denen biometrische Daten (Stimme, Fingerabdruck, Gesichtszüge) gespeichert sind.
- ➔ … automatisch Zugang zu bestimmten Bereichen zugewiesen bekommen, da Identitätsmanagementsysteme im Hintergrund arbeiten und individuelle Berechtigungen erteilen.

Wichtigste Barrieren sind...

- ➔ … Zutritt zum Unternehmen: Ersatz bestehender Systeme.
- ➔ … Zutritt zum Smart Secure Home: Kompatibilität von Zugangskontrolle und digitalen Anwendungen (Smart Home-Konzept), fehlende Standards.

Kritische Faktoren sind...

- ➔ … Akzeptanz im betrieblichen Umfeld: Überwachung, Erfassung von Pausenzeiten, Aufenthalts- und Leistungskontrolle.
- ➔ … Smart Secure Home: Zuverlässigkeit, Bedienerfreundlichkeit, Mehrwert für die Nutzer.

In diesem Szenario stehen der sichere und individualisierte Zugang zu Gebäuden, Räumen, privaten Daten und Unternehmensdaten, Computernetzen und Wissen allgemein sowie die Sicherstellung der Integrität von persönlichen Daten im Mittelpunkt. Mit Hilfe IT-basierter Systeme sollen Dateien und Geräte vor Diebstahl, Manipulation oder Fehlbedienung geschützt werden. Das Ausspähen sensibler persönlicher Daten oder Unternehmensinformationen soll verhindert

werden.

Beim Zutrittsmanagement kommen in Unternehmen, Smart Secure Homes aber auch in Hotels Chipkarten, elektronische Schlüssel und künftig insbesondere RFID-Chips zum Einsatz, auf denen z.B. biometrische Daten (Stimme, Fingerabdruck, 3D-Gesicht) gespeichert sind. Für Zuhause werden in Zukunft die gleichen Sicherheitsvorkehrungen gelten wie im Unternehmen, da zunehmend zentrale Medienserver, so genannte Home Media Networks genutzt werden, die sensible, personenbezogene Daten enthalten, welche von der privaten E-Mail- und Telefonkommunikation über die private Filmsammlung bis hin zu persönlichen Fotoalben reichen.

Beim personalisierten Zugang zu Daten und Dokumenten kommen dagegen Identitätsmanagementsysteme (IMS) zum Einsatz, die automatisch jene Bestände freischalten, die der Nutzer jeweils benötigt und für die er autorisiert ist. Hierfür wird in Zukunft ein einziges Passwort oder eine einzige Chipkarte genügen, da Zugriffsrechte und Freischalteprozeduren zentral gesteuert werden können. Dass dies noch ferne Zukunftsmusik ist, belegt die Unternehmensbefragung zum Einsatz von Identitätsmanagementsystemen (Kapitel 2), die zeigt, dass lediglich 1/5 der befragten Unternehmen derzeit IMS einsetzen.

Bei der individualisierten digitalen Zutrittskontrolle spricht man auch vom „elektronischen Passagierschein“. Als Beispiel führt Cziesche Steffen Fröschle aus Ostfildern an. Dieser hat sich einen RFID-Chip in seine Hand einpflanzen lassen. Jetzt kann er seine Haustür ohne Schlüssel durch bloßes Handauflegen öffnen (Cziesche et al. 2007, S. 68). Solche intelligenten Objekte werden nahezu alle Bereiche des täglichen Lebens beeinflussen, heißt es in der bereits erwähnten Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Wenn aber jede Bewegung Spuren hinterlässt, kann dies tief greifende Auswirkungen auf unser Verständnis von Sicherheit und Privatsphäre haben. Dann ist kaum noch ein Schritt möglich, ohne dass er prinzipiell nachvollziehbar wäre.

Ob als implantierter Chip oder als elektronischer Schlüssel wie beim Auto – die Zutritts- und Routenkontrolle mittels RFID-Systemen wird im Jahr 2020 in öffentlichen, beruflichen und unternehmensinternen Bereichen weit verbreitet sein. Dies beinhaltet auch die vollständige Speicherung der Daten in zentralen Datenbanken. Wesentlich wird die Verbreitung dadurch gefördert, dass Inkompatibilitäten bei geschlossenen Systemen nicht ins Gewicht fallen. Vor allem große Unternehmen, die neue Standorte eröffnen oder die ihre bestehenden IT-Lösungen im Bereich „Zutritt“ erneuern müssen, werden sich für ein RFID-System entscheiden. Unternehmensintern werden RFID-basierte Zutritts- und Routenkontrollen nicht nur im Eingangsbereich von Unternehmensgeländen eingesetzt, sondern auch mit weiteren Funktionen (Zeiterfassung auch zur Ermittlung von Pausenzeiten, Zutritt zu sicherheitsrelevanten Bereichen innerhalb des Geländes, Optimierung von Prozessen und somit Ermittlung auch von personenbezogenen Daten zur Leistungskontrolle). Unternehmen nutzen bereits heute die Möglichkeiten von Informations- und Kommunikationstechnologien zur Verhaltens- und Leistungskontrolle von Erwerbstätigen – auch in Subunternehmen. Nicht immer, so die Einschätzung des BSI, werden Erwerbstätige darüber informiert, dass Informations- und Kommunikationstechnologien zu

Kontrollzwecken eingesetzt werden (BSI 2005, S. 98).

Auch im Freizeitbereich werden sich RFID-Systeme zur Zutrittskontrolle etablieren. Obwohl sie auch zur Routenkontrolle genutzt werden können, steht die Funktion bei der Einführung von RFID-Systemen nicht im Mittelpunkt. Vielmehr wirken die steigende Akzeptanz des Online-Shopping über Internet und Mobilfunk im Bereich des Ticketing sowie der Vorteil, dass Tickets im Verlustfall ersetzt werden können, als Enabler (BSI 2005, S. 98).

Ein vielfach zitiertes Beispiel für den Einsatz von RFID im Freizeitbereich ist die Überwachung von Fußballfans: Eintrittskarten zu Sportgroßveranstaltungen enthalten in Zukunft generell einen RFID-Chip, der einen automatischen Einlass ins Stadion ermöglicht. Einerseits bleiben den Fußballfans so lange Wartezeiten beim Einlass erspart, andererseits wird damit der Schwarzhandel mit Tickets unterbunden. Durch eine zentrale Datenbankanbindung wird gewährleistet, dass im Verlustfall ein neues Ticket ausgestellt und das alte gesperrt werden kann. Die Zuordnung von Ticketnummer zur Person erfolgt bereits beim Vorverkauf und ist nicht veränderbar. Einzig die Besitzer von Geschenktickets müssen sich beim ersten Eintritt ins Stadion in einem separaten Schritt durch Vorlage eines Personaldokuments identifizieren. Das Stadion wird nicht nur im Eingangsbereich, sondern an allen Durchgangspunkten mit Lesegeräten ausgestattet. Diese Vorgehensweise wurde zuvor durch die Allgemeinen Geschäftsbedingungen legitimiert. Die personenbezogenen Daten werden an den Veranstalter, einen privaten Sicherheitsdienst und an die Polizei übermittelt. Letztere hat bereits beim Verkauf der Tickets personalisierte Datenbestände angelegt und ist so jederzeit über den Aufenthaltsbereich von Personen im Stadion informiert, die aus Polizeikontrollen von früheren Anlässen bekannt sind. Auffällig werdende Fanblocks werden als Pulk erfasst, ohne dass die Polizei konfrontative und aufwendige Personenkontrollen durchführen muss. Unbeteiligte Personen, die sich zufällig im Lesebereich der entsprechenden Blocks aufhalten, werden in diesen Fällen allerdings ebenfalls registriert (vgl. BSI 2005, S. 97f).

Digitale Zutrittssysteme bei Unternehmen werden erst allmählich die bestehenden Systeme ersetzen, hier ist mit langen Ersatzzyklen zu rechnen, so dass sich „intelligente“, vernetzte Lösungen nicht so schnell verbreiten dürften wie dies prinzipiell möglich wäre. Auch die Kopplung bestehender IT-Systeme mit Zugangskontrollsystemen stellt eine Herausforderung dar. Der zusätzliche Aufwand, den es bedeutet, solche Systeme zu installieren und in die tägliche Arbeit zu integrieren, dürfte sich zunächst für Unternehmen lohnen, bei denen viele sensible Daten anfallen, deren Verlust zu großen Schäden führen kann.

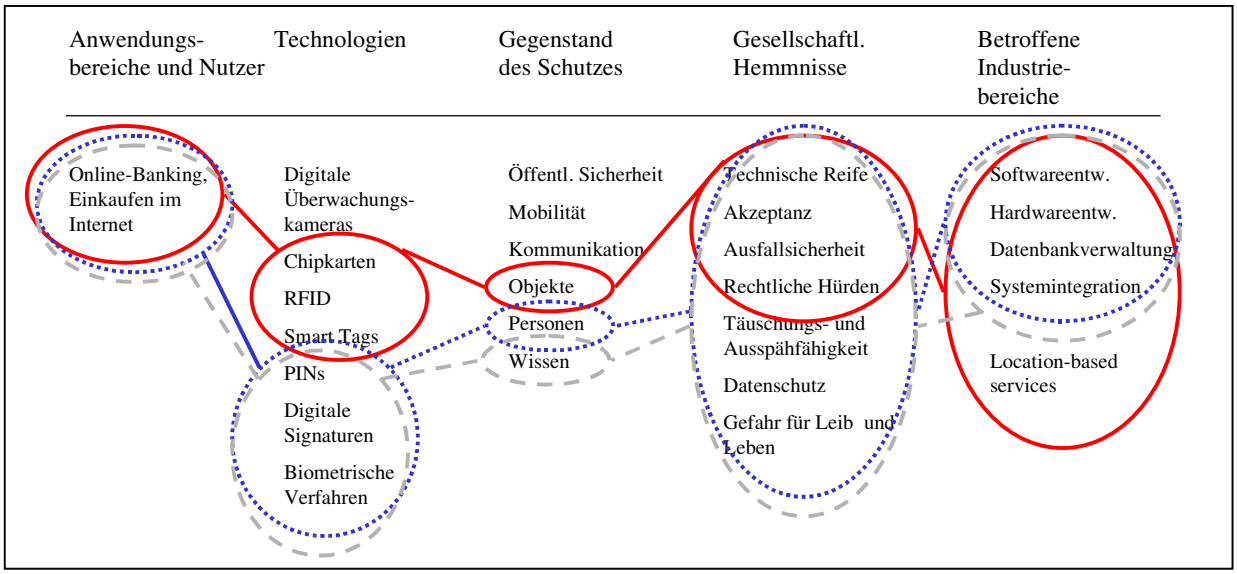
Ein ähnliches Problem besteht heute noch bei der Kopplung von Zugangskontrolle und digitalen Anwendungen im Smart Home. Hier fehlen noch weitgehend Standards und es gibt noch einige Inkompatibilitäten bei Geräten und Systemen. Außerdem mangelt es oftmals noch an Zuverlässigkeit, Bedienerfreundlichkeit und an kommunizierbarem Mehrwert.

Szenario 4: Sicheres Online-Banking und Einkaufen im Internet (inkl. Sicherheit mobiler

Geräte, die erkennen, dass sie gestohlen worden sind)

Das vierte Szenario zeichnet sich durch Kombinationsmöglichkeiten aus, die in Abbildung 24 dargestellt sind.

Abbildung 24: Kombinationen im Szenario: Sicheres Online-Banking und Einkaufen im Internet



2020 werden wir...

- ➔ … sicheres Online-Banking haben und im Internet einkaufen können, ohne befürchten zu müssen, dass persönliche Daten missbraucht werden. Grund: Alle Bürger werden eine digitale Signaturkarte haben, die sie für einzelne Transaktionen authentifiziert.
- ➔ … mobile Geräte nur noch starten und nutzen können, wenn wir diese vorher mit unserem Fingerabdruck freigeschaltet haben.
- ➔ … Verschlüsselungsverfahren haben, die den Zugang Dritter zu persönlichen Daten verhindern. Identitätsdiebstahl wird nicht mehr möglich sein.

Wichtigste Barrieren sind...

- ➔ … digitale Signaturkarten: Die Infrastruktur steht zwar schon heute bereit, aber die Nutzer sind zögerlich und Lesegeräte sind noch nicht weit verbreitet. Usability ist noch ein Problem und der individuelle Mehrwert scheint noch nicht transparent genug.
- ➔ … Fingerscans: Noch nicht schnell genug bei der Erkennung und zu hohe Abweisraten

Kritische Faktoren sind...

- ➔ … wer garantiert die Datensicherheit? Gegenläufiger Trend: Kundendaten für Rabatte.
- ➔ … Akzeptanz der Nutzer.

Die eindeutige Identifikation von Personen beim Kauf von Produkten über das Internet, aber auch bei der Nutzung anderer personalisierter Dienste, ist eine Voraussetzung für sichere Geschäftsabläufe. Hierfür kommen künftig digitale Signaturen und Biometrie-Anwendungen zur Personenidentifikation zum Einsatz. Die Kryptographie als Basistechnologie für die immer

bessere Verschlüsselung von Daten und Kommunikationsinhalten ist ebenfalls ein wichtiger Bestandteil in der Sicherheitslandschaft der Zukunft.

Das Szenario „Sicheres Online-Banking und Einkaufen im Internet sowie der Schutz persönlicher Daten bei Diebstahl von Geräten“ wird genauer bestimmt vom durchgehenden Einsatz folgender Technologien: biometrische Verfahren zur Identifizierung und Zugangskontrolle, „intelligente“ Erkennungsverfahren, PINs, Chipkarten und digitale Signaturen sowie leistungsfähige kryptographische Verfahren.

Interessant ist hier die Feststellung des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien (Bitkom), dass deutsche Unternehmen im Bereich Chipkartentechnologie am Weltmarkt einen Anteil von ca. 70 Prozent des Umsatzes besitzen. Auch im Bereich der Kryptographie haben deutsche Firmen international einen guten Ruf – auch wenn hier nur ein kleiner Marktanteil realisiert wird. Und auch in der Biometrie sind deutsche Firmen in den relevanten Anwendungen mehrheitlich vertreten (Bitkom 2007, S. 19).

Für Online-Banking und für Einkäufe im Internet wird es zunehmend wichtig, sichere Identifizierungs- und Authentifizierungsmechanismen zu verwenden. Zwar gibt es mit der digitalen Signaturkarte schon heute ein Verfahren, das diese Sicherheit gewährleistet, und auch die organisatorische Infrastruktur (Zertifizierungsstellen) ist verfügbar. Allerdings sind die Internetnutzer heute noch sehr zögerlich, digitale Signaturkarten einzusetzen. Nur wenige besitzen überhaupt eine solche Karte. Der Grund hierfür ist, dass Kartenlesegeräte an Computern bisher noch nicht weit verbreitet sind und dass Bedienerfreundlichkeit und Mehrwert heute erst zum Teil gegeben sind.

Auch der Identitätsdiebstahl ist ein relevantes Thema in diesem Zusammenhang. Das Szenario für das Jahr 2020 sieht voraus, dass es bis dahin Verschlüsselungsverfahren gibt, die den Zugang Dritter zu persönlichen Daten unmöglich machen und dass Identitätsdiebstahl technisch nicht mehr möglich ist. Bislang ist es noch relativ einfach, sich im Internet für jemand anderen auszugeben, Einkäufe unter falschem Namen zu tätigen oder anderen Schaden anzurichten. Der Umfang des möglichen Schadens, der mit gestohlenen Identitäten im Internet angerichtet werden kann, steigt mit der Dichte der Vernetzung und dem Stellenwert, den das Internet insgesamt im täglichen Leben und Arbeiten einnimmt. Die Abhängigkeit von IKT-Infrastrukturen und die Gewährleistung eines persönlichen unverfälschten Zugangs werden im Jahr 2020 von noch größerer Bedeutung sein als heute. Hier gibt es eine Überschneidung zum Thema Sicherheit *von* IT bzw. *von* kritischen IKT-Infrastrukturen. Da es in dieser Untersuchung um Sicherheit *durch* IT geht, soll dieser Aspekt hier nicht weiter vertieft werden.

Ein wichtiges Thema ist hier allerdings erneut der Datenschutz bzw. der Umgang der Nutzer mit persönlichen Daten im Internet. Denn auch wenn der Zugang authentisch und sicher ist, heißt dies noch nicht, dass die Nutzer im Internet anonym und unpersönlich agieren können. Im Gegenteil: Die Neigung, private Daten, Produktpräferenzen und andere persönliche Informationen offen zu legen und freiwillig preiszugeben, z.B. um einen Preisvorteil zu erzielen

oder um sich selbst dazustellen (Stichwort Web 2.0), wird in Zukunft weiter zunehmen. In diesem Sinne kann es keine Sicherheit vor Ausspähung privater Daten oder Verwendung der persönlichen Daten durch Unternehmen zum Zwecke des Marketings oder der Krediteinstufung geben, ebenso wie es keine Sicherheit vor staatlicher Kontrolle im Internet geben kann.

In diesem Zusammenhang könnte man auch argumentieren, dass die Vorratsdatenspeicherung von Verbindungs- und Ortsdaten, die im Vorfeld der Verabschiedung des entsprechenden Gesetzes im Frühjahr 2008 kontrovers diskutiert wurde, ein effektives Instrument zur Bekämpfung terroristischer Anschläge oder organisierter Kriminalität ist. Im Szenario 2020 wird davon ausgegangen, dass die juristischen Grauzonen, die es heute noch gibt, um anonymisiert im Internet zu surfen, letztlich beseitigt werden. Dann kann man sich auch nicht mehr für Geld Anonymität erkaufen, indem man einen Remailer oder einen anonymen IP-Server verwendet, um unerkannt E-Mails zu verschicken.

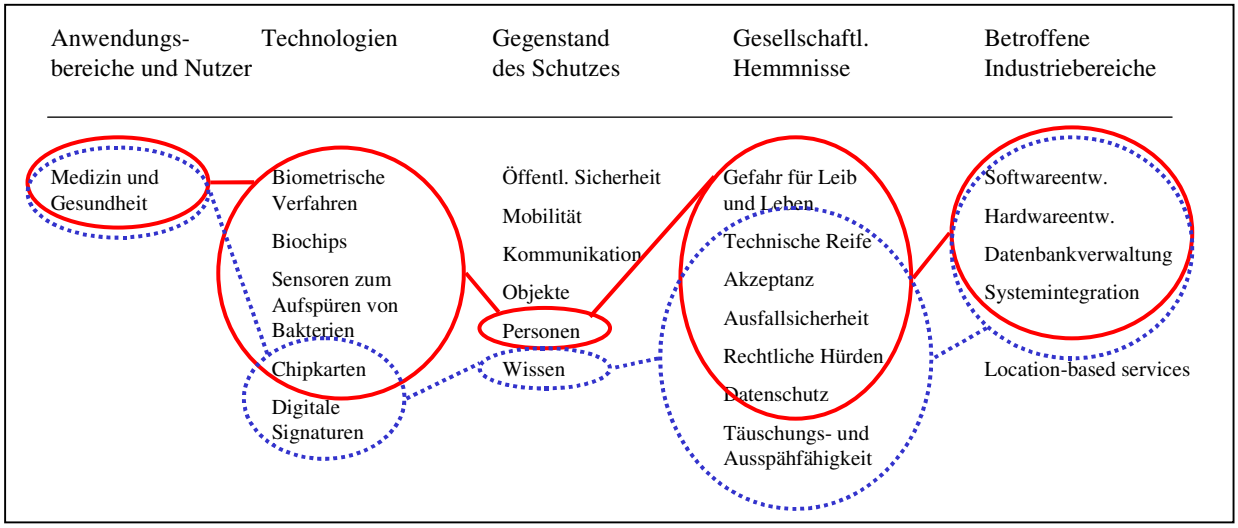
Im Sinne der Leitfrage „Wie kann IT das Leben sicherer machen?“ drängt sich diese Lesart von Sicherheit auf. Umgekehrt könnte man aber auch nach der Sicherheit *vor* IT-basierter Überwachung und Kontrolle fragen und ein Zukunftsbild entwerfen, in dem das Internet von einem Großteil der Menschen nicht mehr genutzt wird, weil es zur vollständigen Überwachung aller Lebensbereiche beiträgt. Die Menschen könnten sich prinzipiell auch immer von dieser kontrollierten Welt abkoppeln und sich den wirtschaftlichen und staatlichen Überwachungsambitionen widersetzen.

Weniger problematisch erscheint dagegen die Erwartung, dass im Jahr 2020 Computer (als Desktop oder als Notebook) und andere mobile Geräte nur noch mit einem Fingerabdruckscanner verkauft werden, womit die Weiterverwendung gestohlener Geräte unmöglich gemacht wird. Die Verwendung von biometrischen Erkennungsmerkmalen stellt nicht nur sicher, dass die mobilen Geräte nur vom rechtmäßigen Besitzer genutzt werden können, sondern auch, dass der Zugang ins Intra- oder Internet nur von dieser Person erfolgen kann. Als Zwischenstufe lassen sich neuartige Nutzererkennungsmechanismen denken, die am Nutzerverhalten erkennen, ob es sich bei dem aktuellen Nutzer um den berechtigten Eigentümer handelt oder nicht, und den Zugriff entsprechend verwehren kann.

Szenario 5: Sicherheit in den Bereichen Medizin und Gesundheit

Das fünfte Szenario zeichnet sich durch Kombinationsmöglichkeiten aus, die in Abbildung 25 dargestellt sind.

Abbildung 25: Kombinationen im Szenario: Medizin und Gesundheit



2020 werden wir...

- ➔ … alle eine Gesundheits-Chipkarte haben, die den Zugriff auf unsere elektronische Patientenakte ermöglicht und die verschiedenen Ärzten abgestuften Zugriff auf unsere Daten ermöglicht.
- ➔ … sicher sein können, dass wir im Krankenhaus die richtige Medikation erhalten, weil ein RFID-Chip im Patientenarmband automatisch die richtige Krankenakte auf den PDA des behandelnden Arztes lädt.
- ➔ … Biosensoren in der Kleidung von Kindern und Älteren einsetzen, um deren Aufenthaltsort und körperliche Verfassung durchgehend überwachen zu können.

Wichtigste Barrieren sind...

- ➔ … Gesundheitskarte: Schneller Zugriff auf zentral verwaltete Daten, Ausfallsicherheit der Server, Verwaltungsstrukturen im Gesundheitssystem.

Kritische Faktoren sind...

- ➔ … Akzeptanz der zentralen Verwaltung von sensiblen Daten bei Ärzten und Patienten. Wer garantiert den Datenschutz? Was passiert bei einem Serverausfall?
- ➔ … Biosensoren: Monitoring ungesunder Essgewohnheiten kann zum Verlust des Versicherungsschutzes führen.

Das Szenario „Sicherheit in Medizin und Gesundheit“ beschäftigt sich mit dem Einsatz der Gesundheitskarte, der sicheren, IT-unterstützten Diagnose im Krankenhaus und in Notfallsituationen sowie mit dem Einsatz von Biosensoren zum Monitoring des Gesundheitszustands.

Das Szenario sieht vor, dass bis zum Jahr 2020 alle Bürger eine Gesundheits-Chipkarte besitzen, mit der sie sich beim Arzt und im Krankenhaus ausweisen können und die zunächst Informationen über ihren Versicherungsschutz enthält. Die Gesundheitskarte verhindert Missbrauch und das Erschleichen von Leistungen und erhöht so die Sicherheit im Gesundheitssystem. Soll-

te es in Zukunft eine Zwei-Klassen-Gesundheitsgesellschaft geben, könnte es sein, dass Versicherungskarten gestohlen oder manipuliert werden, um Behandlungen zu ermöglichen, die der eigene Versicherungsschutz nicht abdeckt. Dadurch würden Sicherheitsaspekte bei der Gesundheitskarte einen noch größeren Stellenwert bekommen.

Neben Informationen zum Versicherungsschutz beinhaltet die elektronische Gesundheitskarte Notfalldaten, wie z.B. die Blutgruppe oder Angaben zum Herzschrittmacher. Über die Karte ist es im Jahr 2020 für entsprechend autorisiertes Personal auch möglich, Zugriff auf die zentral gespeicherte digitale Krankenakte zu erhalten. Der schnelle Zugriff auf individuelle Gesundheitsinformationen (z.B. Allergien, Krankheitsgeschichte usw.) kann gerade in Notfällen lebensrettend sein. Dabei besteht die Herausforderung für das Design von allgegenwärtigen, auf SmartCards basierenden Sicherheits- und Informationskomponenten darin, den Rettungskräften und Ärzten den erforderlichen Informationszugang zu ermöglichen, während zugleich allen anderen Personengruppen ohne ausdrückliche Zustimmung der Betroffenen verwehrt bleiben muss (vgl. Friedewald, Lindner 2007, S. 214).

So wird es im Gesundheitssystem des Jahres 2020 abgestufte Zugriffsrechte auf die elektronische Patientenakte geben. Patienten werden dann z.B. über die Eingabe einer PIN-Nummer beim Arzt geschützte Bereiche offen legen können. Ein Augenarzt, der die Sehstärke prüft, muss beispielsweise nicht über eine bestehende Hepatitis-Infektion Bescheid wissen (Kleinschmidt 2005, S. 77). Auch Apotheker oder Krankenpfleger bekommen nur eingeschränkten Zugriff auf die gespeicherten Daten und können nicht die gesamte digitale Akte einsehen.

Die Vorteile der Gesundheitskarte sind erheblich: Fehlverschreibungen können verhindert werden, weil auf der Gesundheitskarte vermerkt ist, welche anderen Medikamente der Patient noch einnimmt und es wird automatisch geprüft, ob die Wirkstoffe miteinander harmonieren. Sofern das digitale System eine Entlastung der Ärzte von administrativen Aufgaben mit sich bringt, haben die Ärzte mehr Zeit für ihre Patienten. Die Rezepte werden dann nur noch digital ausgestellt, was zur Kostensenkung beitragen kann. Auch Rezeptbetrug ist mit dem System der digitalen Gesundheitskarte so gut wie ausgeschlossen, da die Verschreibung auf einem Server gespeichert wird und vom Apotheker direkt von dort abgerufen wird. Ein weiterer Vorteil der Digitalisierung von Patienteninformationen ist die schnelle Übertragung von Untersuchungsergebnissen per Internet zu Spezialärzten und die Koordinierung von Terminen (Spezialisten, Krankenhauseinweisungen usw.). Weiterhin besteht die Hoffnung auf weniger Doppeluntersuchungen, da die verschiedenen Ärzte eines Patienten die vollständige Krankengeschichte einsehen können und nicht nur über Ausschnitte daraus verfügen (vgl. Kleinschmidt 2005).

Eine wichtige Barriere stellt heute noch der schnelle Zugriff auf die zentral verwalteten Daten dar. Hier müssen technische Lösungen gefunden werden, die die Wartezeiten verringern. Auch die Ausfallsicherheit der Server muss entsprechend sichergestellt werden, denn wenn keine Daten mehr auf Papier existieren, können diese Server für viele Patienten überlebenswichtig sein.

Mit Hilfe unterschiedlicher IT-basierter Systeme kann eine individuelle Medikation von Patienten in Krankenhäusern und im Notfallbereich sichergestellt werden. Hierbei spielen Verfahren des Datenaustausches zwischen Ersthelfer, Krankenwagen und Krankenhaus eine wichtige Rolle. Die Verbindung von Gesundheitskarte, mobilen Lesegeräten und Zugriff auf zentrale Krankenakten im Notfall sowie Weiterleitung der ersten Diagnose aus dem Krankenwagen an das Krankenhaus können hier die Versorgung entsprechend verbessern. Im Krankenhaus selbst kann dann die Medikation – z.B. mit Hilfe von Biosensoren und einem Abgleich digital verfügbarer Daten – an die jeweiligen Bedürfnisse der Person angepasst werden.

Im Krankenhaus des Jahres 2020 werden in großem Stil IT-gestützte Diagnosesysteme eingesetzt. Diese verfügen über elektronisch gespeicherte Fallstudien von Hunderttausenden von Patienten, welche von den Rechnern automatisch durchforstet werden, um verwertbares Wissen zur Verbesserung von Diagnosen zu generieren.

Eine weitere Anwendung von IT im Krankenhaus der Zukunft werden RFID-Armbänder sein. Die so genannten „Funketiketten am Krankenbett“ (eigentlich am Armband des Patienten) tragen dazu bei, die Klinikabläufe effizienter gestalten zu können. Verwechslung und falsche Behandlung können so vermieden werden. Der Arzt kommt bei der Visite mit einem PDA (Personal Digital Assistant), das er in die Nähe des Patientenarmbandes hält, und bekommt die Daten des RFID-Chips übertragen. Daraufhin erscheinen Krankengeschichte und Medikation auf dem Display des PDAs.

Eine wichtige, wenngleich nicht unumstrittene Funktion werden im Jahr 2020 Sensoren und Biochips spielen, die unseren Gesundheitszustand und unser gesundheitsrelevantes Verhalten (Ernährung, Sport usw.) kontinuierlich überwachen. Dabei sind Warnungen vor ungesunder oder gefährlicher Nahrung (etwa bei Allergien) sowie Prognosen über zukünftige Gesundheitsrisiken (z.B. mit Hilfe von Genanalysen) denkbar. Eine weitreichende Vernetzung und die Realisierung verschiedener Komponenten des so genanntem *wearable computing* sind hierfür wichtige Voraussetzungen. Auch diese Anwendung besitzt einen ambivalenten Kern. Funktionskleidung, die mit Sensoren und winzigen Elektroden unsere Körpersignale abtastet und registriert, kann einerseits schnellstmöglich lebensrettende Hilfe rufen. Gleichzeitig könnte eine solche Technologie missbraucht werden, um zu überwachen, wie der Einzelne, gemessen an ökonomischen Maßstäben, mit seiner Gesundheit umgeht. Der Wunsch nach Sicherheit lässt die Implikationen einer solchen Vernetzung leicht verschwimmen. „Wäre es nicht sinnvoll“, fragen z.B. Kersken und Trimbuch, die Autoren eines Gesundheitsszenarios für das Jahr 2057, „wenn die Jacke eines Kindes permanent über den Aufenthaltsort und sein Befinden informierte? Wenn die Kleidung eines alten Menschen bei der Beschleunigung des Herzschlages oder ungewohnten Geräuschen einen Arzt oder Pfleger verständigte? Wie viele Todesfälle wären vermeidbar? Ließen sich kriminelle Übergriffe verhindern? Mit jedem Kindesmissbrauch, jedem wahrgenommenen Unfall steigt die Akzeptanz von Entwicklungen, die unsere Welt sicherer machen, womöglich aber auch kontrollierbarer“ (Kersken und Trimbuch 2007, S. 44f.).

Zusammenfassung und Ausblick

Die Anwendungsszenarien haben gezeigt, dass IT-basierte Zugangs-, Identifikations- und Überwachungssysteme im Jahr 2020 beinahe alle Bereiche durchdringen und omnipräsent sein werden. Die Szenarien haben aber auch gezeigt, dass mit diesen Technologien ganz unterschiedliche Aufgaben erfüllt werden und jeweils unterschiedliche Gegebenheiten berücksichtigt werden müssen. Im Bereich der öffentlichen Sicherheit ging es um Sicherheit vor terroristischen Anschlägen, im Verkehrsbereich ging es umso unterschiedliche Aspekte wie Zugangskontrolle zu Bahnhöfen und Head-up-Displays für Autos; im Unternehmensbereich ging es um den sichereren, individualisierten Zugang zu Unternehmensräumen und -daten und beim Einkaufen über das Internet um die sichere Identifizierung und Authentifizierung. Und zuletzt ging es im Bereich Gesundheit und Medizin um den abgestuften Zugriff auf die Daten der Gesundheits-Chipkarte bzw. auf die digitale Patientenakte.

Es wurde deutlich, dass Sicherheit durch IT nicht ein neuer Markt ist, sondern viele Teilmärkte mit jeweils spezifischen Anforderungen und Einsatzpotenzialen umfasst. Die in dieser Untersuchung getroffene Auswahl von Teilgebieten ließe sich dabei noch erweitern.

Was sich durch alle Anwendungsszenarien gleichermaßen zieht, ist die Bedeutung, die die Akzeptanz der eingesetzten Technologien und Systeme bei den Bürgern, Kunden, Mitarbeitern, Verkehrsteilnehmern oder Patienten hat. Bei der öffentlichen Sicherheit hängt die Akzeptanz von Monitoring- und Überwachungstechnologien von der jeweils aktuellen Bedrohungslage ab. Im Verkehrsbereich hängt sie vom Vertrauen in die Funktionsfähigkeit und von der Bedienerfreundlichkeit ab. Bei den Unternehmen kann sie vom Arbeitgeber mit dem Hinweis auf Effizienzgewinne und unternehmensweit einheitliche Systeme eingefordert werden. Beim Einsatzfeld Smart Secure Home, ebenso wie beim Einkaufen über das Internet, sind Bedienerfreundlichkeit und wahrgenommener Mehrwert ausschlaggebend für die Akzeptanz neuer Zugangstechnologien. Und im Gesundheitsbereich spielt das Vertrauen der Patienten in die Gewährleistung von Datenschutz eine wichtige Rolle. Allerdings ist hier – ähnlich wie im Unternehmensbereich – das Gesundheitssystem in der Lage, Technologien verbindlich einzuführen, die die Patienten schließlich nutzen müssen, ohne dass sie ernsthafte Alternativen haben. Dies zeigt deutlich, dass ausschlaggebend für den Einsatz von IT sein wird, das fragile Gleichgewicht zwischen Nutzen und Ängsten in jedem Anwendungsbereich zu berücksichtigen.

5. Ausblick

Zweifelsohne ist Sicherheit durch IT ein Zukunftsmarkt. In Deutschland allein arbeiten rund 14.000 Wissenschaftler an Technologien, die helfen sollen, Infrastruktur und Bevölkerung zu schützen. Der Markt für Sicherheitstechnik wächst hier jährlich um sieben bis acht Prozent, Tendenz steigend. Zum ersten Mal hat die Bundesregierung 2007 ein Förderprogramm für zivile Sicherheitstechnik verabschiedet. Bis 2011 sollen 123 Millionen Euro in die Entwicklung von Technologien fließen, die „Sicherheit bieten, aber unsere Freiheit nicht beeinträchtigen", so der Beschluss[7]. IT als Querschnittstechnologie ist bereits heute zentral in der Umsetzung von Sicherheitskonzepten, da die relevanten Endgeräte immer stärker IT-basiert agieren. Es ist davon auszugehen, dass IT-basierte Zugangs-, Identifikations- und Überwachungssysteme weiter an Bedeutung zunehmen werden und sich vielversprechende Marktchancen bieten.

Treiber für diese Entwicklung sind einerseits regulatorische Änderungen und Auflagen, die die Nutzung bestimmter Technologien im Rahmen von Sicherheitskonzepten zwingend machen. Gleichzeitig wird aber auch Vertrauen zunehmend zu einer wichtigen Ressource für Geschäftserfolg – gerade bei hochgradig sensiblen Geschäftsvorgängen im Bank- und Versicherungsgewerbe, aber auch bei Transaktionsvorgängen. Sicherheit durch IT kann dieses Vertrauen erzeugen – der Einsatz entsprechender zuverlässiger Systeme vorausgesetzt.

Zum Thema Datenschutz könnte der Status Quo in Deutschland schon bald eine Wende erleben. Zumindest wenn man dem Soziologen Ronald Hitzler von der Technischen Universität Dortmund Glauben schenkt, der meint, dass die Diskussion über Opfer und Bespitzelung aufgelöst wird in die des Voyeurismus: „Wir leben in einer Gesellschaft, in der man ständig auf sich aufmerksam machen muss, im Job, im Privatleben, wir verwandeln uns in Ego-Manager einer Ökonomie der Aufmerksamkeit." (Die Zeit, 2008, S. 58). Überwachung in der modernen Gesellschaft ist eben nicht wie früher nur mit unbehaglichen Gefühlen verbunden, sondern auch mit einem Interesse an Sicherheit und einem Wunsch nach Beachtung.

Dieser Band der FAZIT-Schriftenreihe hat das Thema „Sicherheit durch IT" am Beispiel Baden-Württemberg anhand von drei Perspektiven untersucht: dem Einsatz von Identitätsmanagementsystemen in baden-württembergischen Unternehmen, dem Einsatz von IT-Systemen zur Gewährleistung von Gebäudesicherheit im öffentlichen Raum am Beispiel des Flughafens Stuttgart sowie durch eine Szenario-Analyse zum Einsatz von IT-basierten Sicherheitstechnologien in verschiedenen Anwendungskontexten in Baden-Württemberg im Jahr 2020.

[7] Vgl. www.ideen-zuenden.de

Wie jede andere Technologie auch, zum Beispiel das Auto, das Telefon oder das Internet, weckt Identitätsmanagement seit den Anfangstagen Bedürfnisse und Interessen, die vor dem Entstehen der Technologie in diesen Ausmaßen eigentlich unbekannt waren. Zunächst ging es um einfache Authentifizierung mittels Passwörtern und Zugriffskontrolle. Inzwischen gehören Multi-Faktor-Authentifizierung, Biometrie und Federated Identities zum Repertoire. Aber, wie bei allen anderen großen Technologien auch, ist das Ende der Fahnenstange noch lange nicht erreicht. Mit dem zunehmenden Einsatz und der Verbreitung von Identitätsmanagement wachsen die Anforderungen, denen sich die Technologie anpassen muss. Aktuell stehen Rollen und Rechte im Vordergrund sowie Genehmigungsprozesse und deren Dokumentation. Jeder kann so nur gemäß seiner Rolle auf Unterlagen und Systeme zugreifen. Die Sicherheitsrisiken, die Unternehmen aus eigenen Reihen drohen, werden dadurch minimiert. Der ursprüngliche Fokus verschiebt sich bereits auf die Anwendungen, aber es geht nach wie vor um Authentifizierung und Autorisierung. Die Herausforderungen, die damit gelöst werden, ändern sich in der nahen Zukunft. Wieso? Identitätsmanagement-Systeme sind die besten Depots für Informationen über ihre Nutzer. Mit diesen Informationen lässt sich weitaus mehr machen, als lediglich Nutzer verwalten und in Gruppen einteilen. Compliance-Systeme können zum Beispiel Identitäten nutzen, um Richtlinien einzuhalten und webbasierte Anwendungen können unter Verwendung der Identitäts-Informationen personalisierte Dienste anbieten. Dabei gilt: Je mehr Informationen die Anwendungen über ihre Nutzer haben, desto besser können sie personalisiert zur Verfügung stehen. Durch Identitätsmanagement als Service-basiertes Modell können Anwendungen leichter Informationen über Identitäten verwenden. Gleichzeitig werden die Administration und der Zusammenschluss von Identitäten (Federation) vereinfacht und so Identitätsmanagement schneller, besser und kostengünstiger. Es wird also einen Paradigmenwechsel geben, weg vom Fokus auf Authentifizierung hin zu einem Fokus auf verschiedene Services, die Identitätsmanagement-Systeme den Anwendungen über eine konsistente Oberfläche zur Verfügung stellen. Das heißt, es wird weniger um die Technologie gehen, die Zugriffe, Zugänge und Zutritte regelt, sondern viel mehr darum, was mit den Identitäten gemacht werden kann. Dieser Blick in die Zukunft sollte allerdings auch kritisch geerdet werden mit den Erkenntnissen aus der FAZIT Unternehmensbefragung, die belegt, dass Identitätsmanagementsysteme bislang nur für bestimmte Branchen eine Relevanz gewinnen konnten, zudem fast ausschließlich für große Unternehmen und zum Management der eigenen Mitarbeiter. Hier bleiben also Potenziale noch wesentlich unausgeschöpft.

Dennoch zeigen die Ergebnisse dieses Bandes auch auf, dass Sicherheit durch IT kein einheitlicher und abgrenzbarer Markt ist, sondern aus vielen Einzeltechnologien besteht, die sehr unterschiedliche Aufgaben erfüllen und auf jeweils unterschiedliche Gegebenheiten angepasst sind. So sind die Sicherheitssysteme am Flughafen Stuttgart zum Beispiel sehr speziell und vor allem aufgrund von regulatorischen Auflagen eingesetzt, auf die der Flughafen nur begrenzt Einfluss hat. In der konkreten Übersetzung der Auflagen in den Kauf einzelner Systeme allerdings hat der Flughafen großen Spielraum und setzt diesen auch ein. Die Entwicklungen in dem Bereich sind rasant – bedingt auch durch entsprechende Fördermittel. So zum Beispiel wird derzeit eine bahnbrechende Sicherheitstechnologie im Rahmen des von der EU geförder-

ten Projekts TeraSec[8] erforscht: Mit Terahertz-Wellen, die im Frequenzbereich zwischen Mikrowellen- und Infrarotstrahlung zu finden sind, werden viele Stoffe transparent. Gleichzeitig ist nach heutigem Wissensstand die schwache Strahlung, die nicht in tiefere Gewebeschichten vordringt, für den Menschen unschädlich. Mit dieser Technologie lässt sich den Menschen quasi unter die Kleidung sehen und dort versteckte Gegenstände erkennen. Im Sektor Sicherheitssysteme für öffentliche Räume werden – bereits in der nahen Zukunft - noch weitere Innovationen zu erwarten sein.

Auch die Zukunftsszenarien haben vor Augen geführt, dass Sicherheit durch IT sehr unterschiedliche Aspekte wie die Sicherheit vor terroristischen Anschlägen, Zugangskontrollen oder sichere Authentifizierung und Identifizierung berührt. Dementsprechend muss Sicherheit durch IT nicht als ein neuer Markt, sondern als eine Vielzahl von Teilmärkten mit jeweils spezifischen Anforderungen und Einsatzpotenzialen verstanden werden. Wolle man erreichen, dass Sicherheitsstechnologien gesellschaftlich und juristisch akzeptiert würden, so der Chef des Fraunhofer-Instituts IITB Jürgen Beyerer, „müssen in Zukunft Geisteswissenschaftler von Anfang an in die Forschungen und Diskussionen mit eingebunden werden.“ (Die Zeit, 2008, S. 61). Denn neben all den Zukunftsperspektiven des Marktes für Sicherheit durch IT muss eines immer klar sein: Sicherheit hat auch seinen gesellschaftlichen Preis, der stetig ausgehandelt wird.

[8] Vgl. http://solarsystem.dlr.de/terasec

6. Literatur

Aschenbrenner, Norbert (2005): Elektronischer Scharfsinn. In: Pictures of the Future, Herbst, Siemens. S. 43-45.

Bertschek, Irene; Döbler, Thomas (Hrsg) (2005): Open Source Software und IT-Sicherheit. Unternehmensbefragung Frühjahr 2005 in Baden-Württemberg. FAZIT-Schriftenreihe, Band 1, Juli 2005. Stuttgart/ Mannheim: MFG/ ZEW.

Bertschek, Irene; Müller, Bettina; Ohnemus, Jörg; Schleife, Katrin; Schmidt, Tobias (2006): E-Business in Baden-Württemberg. Unternehmensbefragung im Juni/Juli 2006. FAZIT-Schriftenreihe, Band 4, November 2006. Stuttgart/ Mannheim: MFG/ ZEW.

Bertschek, Irene; Engelstätter, Benjamin; Müller, Bettina; Ohnemus, Jörg; Vogelmann, Tobias (2008): Unternehmenssoftware und Eingebettete Systeme. Unternehmensbefragung Herbst/Winter 2007 in Baden-Württemberg. FAZIT-Schriftenreihe, Band 11, Mai 2008. Stuttgart/ Mannheim: MFG/ ZEW.

BITKOM (2007): IT, Telekommunikation und neue Medien in Deutschland. Lage und Perspektiven der Branche. Handlungsempfehlungen für eine strategische Innovations- und ITK-Politik. Ein Thesenpapier. www.bitkom.org/files/documents/Thesenpapier_ BITKOM_Innovations-_und_ITK-Politik_07-2005.pdf

Blind, Knut; Gauch, Stephan; Goluchowicz, Kerstin (2007): Identifikation zukünftiger Standardisierungsfelder. Projekt des DIN zur Förderung der Innovation und Marktfähigkeit durch Normung und Standardisierung (INS). Gefördert durch das BMWi. Lehrstuhl für Innovationsökonomie der Technischen Universität Berlin in Kooperation mit dem Fraunhofer ISI, Karlsruhe. 2. Auswertungswelle, Juni. Fragebogen Online: www.interest.isi.fraunhofer.de/din_ins/sec

Buller, Ulrich (2006): Forschung für Security: Sicherheit und Schutz durch Technologie und Innovation. Dokumentation des Vortrages auf dem Fraunhofer-Symposium „Future Security“ am 4./5. Juli 2006 in Karlsruhe. Online: www.vvs.fraunhofer.de/ de/downloads/future-security.htm

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2005): Risiken und Chancen des Einsatzes von RFID-Systemen. Online: www.bsi.bund.de/fachthem/rfid/ RIKCHA_barrierefrei.pdf.

Cziesche, Dominik; Ulrich, Andreas; Verbeet, Markus (2007): Total unter Kontrolle. In: Spiegel Spezial Nr. 3: Wir sind das Netz, S. 64-69.

Die Zeit Wissen (2008): Technik gegen den Terror, Nr. 4, S. 54-61.

Eckert, Claudia (2004): IT-Sicherheit: Konzept – Verfahren – Protokolle. München, Wien.

Friedewald, Michael; Lindner, Ralf (2007): Datenschutz, Privatsphäre und Identität in intelligenten Umgebungen: Eine Szenarioanalyse. In: Mettern, Friedemann (Hrsg.): Die Informatisierung des Alltags: Leben in smarten Umgebungen. Berlin: Springer, S. 207-231.

Gerl, Bernhard (2004): Permanenter Reifen-Service. In: Pictures of the Future, Herbst, Siemens. S. 65.

Grasemann, Gunther (2000): Videosensorik wird zuverlässiger. In: WIK. Zeitschrift für Wirtschaft, Kriminalität und Sicherheit 22, Nr.2, S. 54-55.

Grasemann, Gunther. (2007a): Reference Architecture for protection systems. In: Beyerer, J. (Hg.): Future security. 2nd Security Research Conference 2007: 12th-14th September, Karlsruhe, Germany. Karlsruhe: Universitätsverlag Karlsruhe, 2007, S. 128-130.

Grasemann, Gunther. (2007b): Integrierte Sicherheit. In: visit 1/2007. Karlsruhe: Fraunhofer Institut Informations- und Datenverarbeitung (IITB), S. 4-5.

Haller, Steffen (2005): Integriertes Gebäudemanagement durch offene Gebäudeautomation. In: Bundesindustrieverband Heizungs-, Klima-, Sanitärtechnik/ Technische Gebäudesysteme e.V. (Hg.): BHKS-Almanach 2005. Bonn: TGC – Technische Gebäudeausrüstung Consulting GmbH, S. 57-60.

Hassenmüller, Harald (2007): Unbeschwert reisen. In: Pictures of the Future, Herbst, Siemens. S. 100-102.

Horn, Marion (2007): Besser schützen. In: Fraunhofer Magazin Nr. 4, S. 36-37.

IPTS (2005): Biometrics at the Frontiers: Assessint the Impact on Society. For the European Parliament Committee on citizens´ Freedoms and Rights, justice and Home Affairs (LIBE), European Commission, DG Joint Research Centre, February, Seville: IPTS.

Kerbusk, Klaus-Peter (2007): Klick, du bist tot. Über Virenepedemien, Kontenklau und Identitätsdiebstahl. In: Spiegel Spezial Nr. 3: „Wir sind das Netz“. Wie das neue Internet die Gesellschaft verändert“, S. 91-97.

Kersken, Uwe; Trimbuch, Sonja (Hrsg.) (2007): 2057. Unser Leben in der Zukunft. Autoren: Olsberg, Karl; Ruby, Claudia; Marquardt, Ulf. Leipzig: Aufbau Verlag.

Kleinschmidt, Andreas (2005): Der lombardische Patient. In: Pictures of the Future, Herbst, Siemens. S. 76-79.

Lüders, C.: Teilnehmende Beobachtung. In: Bohnsack, R.; Marotzki, W.; Meuser, M. (Hrsg.) (2003): Hauptbegriffe Qualitativer Sozialforschung. Opladen, S.151-153

Müller, Klaus-Reiner (2005): Handbuch Unternehmenssicherheit. Umfassendes Sicherheits-, Kontinuitäts- und Risikomanagement mit System. Wiesbaden: Vieweg.

Niesing, Birgit (2007): Sicherheit durch Hightech. In: Fraunhofer Magazin 3, S. 8-12.

Oertzen, Jürgen von; Cuhls, Kerstin; Kimpeler, Simone (2006): Wie nutzen wir Informations- und Kommunikationstechnologien im Jahr 2020? Ergebnisse einer Delphi-Befragung. FAZIT-Schriftenreihe, Band 3, April 2006. Stuttgart/ Karlsruhe: MFG/ Fraunhofer ISI.

Palensky, P. et. al. (2006): Netzwerke und Gebäude. In: e & i Elektrotechnik und Informationstechnik. Volume 123, Number 6 / Juni 2006, Wien, S. 259-268.

Pease, Arthur F. (2004): Das Programm des Lebens. In: Pictures of the Future, Herbst, Siemens. S. 38-41.

Pease, Arthur F. (2006): Maschinen lernen sehen. In: Pictures of the Future, Herbst, Siemens. S. 83-86.

Pfitzmann, Andreas (2006): Biometrie – Wie einsetzen und wie keinesfalls? In: Informatik-Spektrum, Volume 29, Nummer 5, Oktober 2006. Berlin/Heidelberg: Springer.

Roco, Mihail C.; Bainbridge, William Sims (eds.), 2002: Converging Technologies for Improving Human Performance. Nanotechnology, Biotechnology, Information Technology and Cognitive Science. Reoprt sponsored by the National Science Foundation and the US Department of Commerce. Arlington, VA, June 2002

Schleife, Katrin; Schmid, Oliver (2005): IT-Sicherheit in Unternehmen. In: Bertschek, Irene; Döbler, Thomas (Hrsg.): Open Source Software und IT-Sicherheit. Unternehmensbefragung Frühjahr 2005 in Baden-Württemberg. FAZIT-Schriftenreihe, Band 1, Juli 2005. Stuttgart/ Mannheim: MFG/ ZEW, S. 81-99.

Schröder, Tim (2005): Funketikett am Krankenbett. In: Pictures of the Future, Herbst, Siemens. S. 82.

Steinmüller, Karlheinz (2006): Die Zukunft der Technologien. Mit Angela Steinmüller. Hamburg: Murmann.

Trage, Sylvia (2006a): Sensible Strukturen. In: Pictures of the Future, Frühjahr, Siemens. S. 32-33.

Trage, Sylvia (2006b): Bildverarbeitung im Aufwärtstrend. In: Pictures of the Future, Herbst, Siemens. S. 93.

Wohllaib, Nicola (2007): Vernetztes Zuhause: Willkommen im Smart Home. In: Pictures of the Future, Herbst, Siemens. S. 86-88.

Internetquellen

www.fazit-forschung.de

www.doit-online.de

www.mfg-innovation.de

www.emi.fraunhofer.de/EMI-Links/InnovationsclusterFutureSecurityBW/

www.sicherheitsforum-bw.de

www.flughafen-stuttgart.de

www.hightech-strategie.de

www.cordis.eu

www.security-messe.de

www.ideen-zuenden.de

7. Autoren-, Projekt- und Partnerinformation

Über die Autoren

Beckert, Bernd, Dr. phil. ist Projektleiter beim Fraunhofer Institut System- und Innovationsforschung (ISI) in Karlsruhe. Seine Spezialgebiete sind interaktive Medien über unterschiedliche technische Plattformen, die Analyse organisatorischer und wirtschaftlicher Veränderungsprozesse durch den Einsatz von IKT in Unternehmen und die Evaluierung regulativer Vorgaben und Fördermaßnahmen auf die Verbreitung von IKT. Seit Januar 2008 ist er stellvertretender Leiter des Competence Centers Neue Technologien beim Fraunhofer ISI. Bernd Beckert studierte Politikwissenschaft, Soziologie und Amerikanistik an der Universität Konstanz und der Portland State University in Oregon, USA. Von 1997-2000 war er wissenschaftlicher Mitarbeiter in der Forschungsgruppe Telekommunikation der Universität Bremen.

Buchholz, Andrea, Dr. phil. ist seit 2007 Projektleiterin von FAZIT Forschung bei der MFG Stiftung Baden-Württemberg. Ihr Arbeitsschwerpunkt ist neben dem Projekt- auch das Forschungsmanagement. Andrea Buchholz studierte Informatik (Universität Hamburg) und Künstliche Intelligenz (University of Edinburgh) und promovierte in Techniksoziologie mit dem Schwerpunkt Benutzerfreundlichkeit neuer Technologien (Brunel University, London). Von 2002-2004 arbeitete sie bereits für die MFG Medien- und Filmgesellschaft Baden-Württemberg als Projektleiterin der europäischen E-Content Initiative ACTeN.

Goluchowicz, Kerstin, Dipl.-Math. oec. ist seit 2006 wissenschaftliche Mitarbeiterin am Lehrstuhl für Innovationsökonomie des Instituts für Technologie und Management der Technischen Universität Berlin und des Competence Center „Regulierung und Innovation“ des Fraunhofer ISI in Berlin. Zu ihren Forschungsschwerpunkten gehören Forecast-Methoden für die Innovationsforschung, Methoden zur Innovations- und Technologiebewertung sowie der Methodenentwicklung für die Szenario- und Delphi-Analyse. Kerstin Goluchowicz studierte Wirtschaftsmathematik an der Technischen Universität Berlin mit den Nebenfächern Marketing sowie wirtschafts- und verwaltungsorientierte Anwendungen der Informatik.

Hartmann, Bernd arbeitet seit 2008 als freier Berater für die Kreativwirtschaft. Schwerpunkte seiner Arbeit sind Digital Content, Innovationskommunikation und Social Software. Bernd Hartmann studierte Journalistik, Germanistik und Betriebswirtschaftslehre an der Universität Bamberg und der University of Waterloo (Kanada). Von 2004 bis 2007 arbeitete er bei der MFG Medien- und Filmgesellschaft Baden-Württemberg, zuletzt als Projektleiter International Affairs. 2007 wechselte er als Consultant zur Berliner Unternehmensberatung Goldmedia Consulting & Research.

Über FAZIT Forschung

FAZIT (Forschungsprojekt für aktuelle und zukunftsorientierte Informations- und Medientechnologien und deren Nutzung in Baden-Württemberg) identifiziert seit 2005 neue Märkte für innovative Informations- und Kommunikationstechnologien und erforscht bis Anfang 2009 Perspektiven zukünftiger IT- und Medienentwicklung von regionaler Bedeutung.

Am Beispiel Baden-Württemberg beschreitet FAZIT neue Wege und kombiniert qualitative Forschung mit statistischen Erhebungen. Das Forschungsspektrum reicht von Marktanalysen und Unternehmensbefragungen über Fallstudien und wissenschaftliche Workshops bis hin zu Delphi-Studien, Szenarioprozessen und Roadmapping. FAZIT hat 15 relevante Schwerpunkthemen erkannt und präsentiert dazu kontinuierlich Forschungsergebnisse, die durch eine ausgeprägte Transferkomponente Impulse für weitere Forschung und Entwicklung geben.

Projektträger von FAZIT ist die MFG Stiftung Baden-Württemberg in Stuttgart. Partner sind das Zentrum für Europäische Wirtschaftsforschung (ZEW) in Mannheim und das Fraunhofer-Institut für System- und Innovationsforschung (Fraunhofer ISI) in Karlsruhe.

Mehr Informationen im Internet unter www.fazit-forschung.de

Über die Partnerinstitutionen

MFG Stiftung Baden-Württemberg
Die MFG Stiftung wurde 2003 ins Leben gerufen. Ziel ist Aus- und Weiterbildung sowie Förderung von Kunst, Kreativität und Kultur. Schwerpunkte sind Forschung und Entwicklung in den Bereichen Medien, IT und Film im Rahmen eigener Projekte. Die MFG Siftung fördert innovative Projekte und Forschungsaktivitäten durch Studien, Stipendienprogramme sowie Wettbewerbe. Darüber hinaus bietet sie neue Fort- und Weiterbildungsangebote an und vernetzt Akteure im Bildungs- und Forschungsbereich. Internet: www.mfg.de/stiftung

Fraunhofer-Institut System- und Innovationsforschung
Das Fraunhofer-Institut für System- und Innovationsforschung (ISI), untersucht Entstehungsbedingungen und Märkte innovativer technischer Entwicklungen und deren Auswirkungen auf Wirtschaft, Staat und Gesellschaft. Die Forschungsgruppen konzentrieren sich auf neue Technologien, Industrie- und Serviceinnovationen, Energiepolitik und nachhaltiges Wirtschaften sowie auf Dynamik regionaler Märkte und Innovationspolitik. Internet: www.isi.fraunhofer.de

Zentrum für Europäische Wirtschaftsforschung
Das ZEW arbeitet auf dem Gebiet der anwendungsbezogenen empirischen Wirtschaftsforschung. Methodisch sind die Arbeiten primär mikroökonomisch und mikroökonometrisch ausgerichtet. Die Forschungsgruppe Informations- und Kommunikationstechnologien (IKT) am ZEW befasst sich mit den Entwicklungen und den Auswirkungen der zunehmenden Verbreitung von IKT, wobei der Fokus insbesondere bei industrie- und arbeitsmarktökonomischen Fragestellungen liegt. Hierzu gehören beispielsweise die Auswirkungen der IKT-Nutzung auf Produktivität, Innovation, Unternehmensorganisation und Unternehmenswachstum sowie auf die Anforderungen an die Qualifikation der Beschäftigten. Internet: www.zew.de

PROJEKTTRÄGER

MFG Stiftung Baden-Württemberg

PARTNER

Fraunhofer ISI Institut System- und Innovationsforschung

ZEW Zentrum für Europäische Wirtschaftsforschung GmbH