booz&co.

Bundesministerium für Wirtschaft und Technologie

Die IT-Sicherheitsbranche in Deutschland -

Aktuelle Lage und ordnungspolitische Handlungsempfehlungen

Endbericht

Stand: 16.2.2010

Dr. Rainer Bernnat

Marcus Bauer

Dr. Wolfgang Zink

Dr. Nicolai Bieber

Dietmar Jost

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Zusammenfassung der Ergebnisse und Handlungsempfehlungen

Mit der vorliegenden Studie „Die IT-Sicherheitsbranche in Deutschland – Aktuelle Lage und ordnungspolitische Handlungsoptionen“ hat das Bundesministerium für Wirtschaft und Technologie (BMWi) Booz & Company beauftragt, die IT-Sicherheit in Deutschland, als signifikanten Teil des gesamten Marktes für Informationstechnologie, einer aktuellen und zusammenfassenden Untersuchung aus Standortperspektive zu unterziehen und Handlungsoptionen für das BMWi abzuleiten.

Die Informations- und Kommunikationstechnologie (IKT) gehört zur kritischen Infrastruktur und hat sich angesichts der zunehmenden Vernetzung vieler lebenswichtiger Systeme und Funktionen zu einem zentralen Nervensystem des Landes entwickelt. Zudem durchdringt die Informationstechnologie in steigendem Maße den beruflichen und auch den privaten Alltag („ubiquitous computing“). Mit der immer größeren Bedeutung der IKT sowie der nicht geringer werdenden Zahl von Sicherheitslücken, steigen auch die Bedrohungen für die IKT. In den letzten Jahren ist dabei eine zunehmende Professionalisierung der Angriffe sowie der eingesetzten Schadprogramme und Werkzeuge zu beobachten. Aus dieser Gesamtlage heraus ergibt sich eine zentrale und äußerst wichtige Aufgabe der IT-Sicherheit für die Wahrung der nationalen Sicherheit sowie für den Schutz von persönlichen Daten und Unternehmensdaten.

Angesichts der Schutzbedarfe hat sich ein umfangreiches Angebot für IT-Sicherheitsprodukte und -dienstleistungen entwickelt. Die verfügbaren Hochrechnungen zu Marktgröße und -wachstum unterscheiden sich nach Segmentierung und Analyseperspektive deutlich. In einer vorsichtig konsolidierten Betrachtung geht die vorliegende Studie von einer geschätzten weltweiten Marktgröße für IT-Sicherheit von rund 33 Mrd. Euro aus. Das voraussichtliche durchschnittliche Wachstum in den Jahren 2009 bis 2012 beläuft sich auf etwa 13,4% im Jahresschnitt. Als Markt bleibt IT-Sicherheit damit trotz Wirtschafts- und Finanzkrise sehr attraktiv. Auch in Deutschland hat IT-Sicherheit mit einem plausibilisierten Umsatzvolumen von rund 2,5 Mrd. Euro und einem prognostiziertem Wachstum von ca. 10% eine signifikante Marktgröße erreicht und weist ein im Vergleich zu den meisten anderen Branchen über-

durchschnittliches Wachstum auf. Allerdings bleibt der Markt in Deutschland deutlich unterhalb der Steigerungsraten des Weltmarkts.

Die deutschen Anbieter im Bereich IT-Sicherheit werden, auch für die Zukunft, grundsätzlich als wettbewerbsfähig im internationalen Markt eingestuft. Es fällt jedoch auf, dass in Deutschland, mit Ausnahme von T-Systems und Giesecke & Devrient hauptsächlich kleine spezialisierte Anbieter ansässig sind, die einen Jahresumsatz von deutlich weniger als 100 Mio. Euro erwirtschaften.

Im direkten Vergleich der deutschen IT-Sicherheitsanbieter mit den weltweit führenden Unternehmen dieser Branche in Bezug auf Umsatz mit IT-Sicherheitsprodukten und –dienstleistungen und Zahl der Mitarbeiter wird der Abstand zur Weltspitze deutlich (vgl Abbildung 1). Die weltweit führenden Unternehmen sind Kooperations- und Vertriebspartnerschaften mit den führenden PC-Herstellern eingegangen und konnten dadurch den Massenmarkt über globale Vertriebs- und Servicenetze besetzen. Die Studie kommt dabei zu dem Schluss, dass für die deutschen Unternehmen der Massenmarkt nicht adressierbar ist, sollte es ihnen nicht gelingen, entsprechende Kooperationen zum Aufbau internationaler Vertriebsnetze einzugehen.

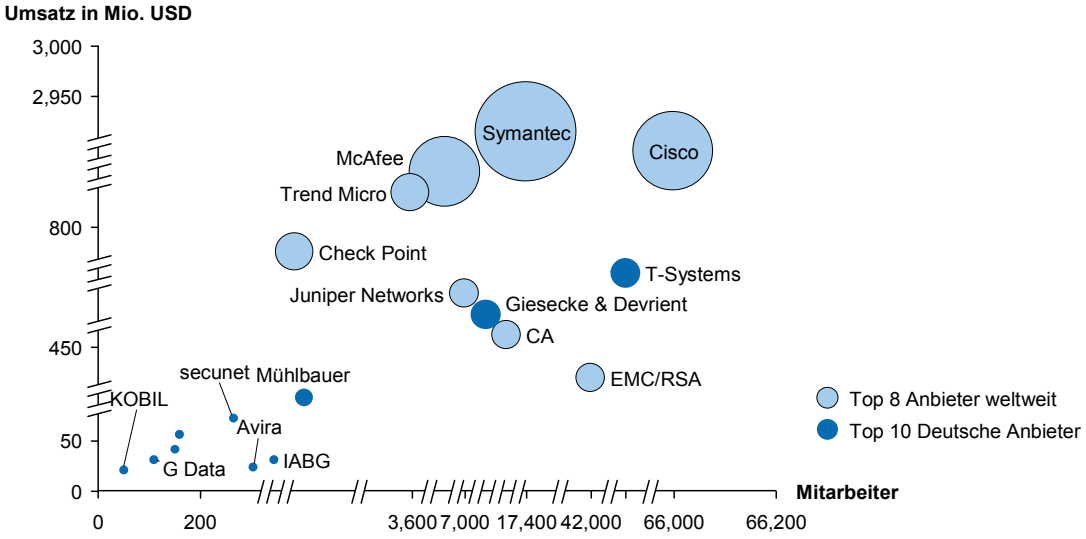


Abbildung 1: Vergleich deutscher Anbieter von IT-Sicherheit mit weltweit führenden Unternehmen nach Umsatz in Mio. US-Dollar (2007) und Gesamtzahl der Mitarbeiter[1]

Die Stärken und Schwächen der deutschen IT-Sicherheitsanbieter und ihres Umfelds wurden bei der Analyse im wesentlichen in drei Handlungsziele

[1] IDC 2009, Booz & Company Analyse

eingeordnet: *Sicherung kritischer Kompetenz*, *Innovation* und *Wachstum*. Diese Gliederung wurde im weiteren Verlauf der Studie für die Formulierung der ordnungspolitischen Handlungsoptionen fortgeführt. Trotz der erfreulichen Stärke der IT-Sicherheitsbranche sind strukturelle Schwächen vorhanden, die dazu führen, dass die Branche im internationalen Vergleich zurückfällt (vgl. Tabelle 1). Als eine besondere Stärke der IT-Sicherheitsbranche kann indes hervorgehoben werden, dass das Thema mit deutscher Ingenieurskunst und Gründlichkeit in Verbindung gebracht wird. Zudem genießen deutsche Hersteller eine hohe Reputation, da für deutsche Technologie im Ausland eine verlässliche Neutralität angenommen wird. Die entwicklungsseitige Vorreiterrolle, insbesondere im Bereich der Kryptographie, sowie die Herkunftsbezeichnung „Made in Germany" sind für die deutschen Anbieter im internationalen Markt für IT-Sicherheit sehr gute Differenzierungsmerkmale.

Tabelle 1: Übersicht der wichtigsten Stärken und Schwächen des deutschen IT Sicherheitsmarkts geordnet nach Handlungszielen

AUSWAHL

	Sicherung	Innovation	Wachstum
Stärken	+ Hohes Ansehen des Bundesamts für Sicherheit in der IT (BSI) + BSI-Zertifizierung international anerkannt	+ Hoher Technologiestandard + Hochwertige Fachkräfteausbildung	+ Positives Image "Made in Germany" + Hohes Vertrauen in Deutschland im Ausland + Starke Kompetenzbereiche
Schwächen	- Lücken in kritischen Kompetenzen - Keine vollständige "nationale Werkbank" - Geringe Einflussnahme auf internationale Standards	- Zu geringe Berücksichtigung internationaler Standards - Vorbildfunktion des Staates wenig ausgeprägt - Geringe Exzellenzförderung - Unklare Zielsetzung bei Großprojekten - Zu wenig Awareness	- Hoher Anteil an kleinen und mittleren Unternehmen (KMU) - Ausbaubedarf bestehender Exportunterstützung für KMU - Schwache Kooperation innerhalb der Wirtschaft - "time-to-market" zu lang - Zu hohe Abhängigkeit von Staatsaufträgen - Schwacher Kapitalmarkt

Allerdings hat die Analyse auch deutliche Schwächen des deutschen IT-Sicherheitsmarkts im internationalen Wettbewerb aufgedeckt. Zu nennen sind die vergleichsweise kleingliedrige Struktur der deutschen Anbieterseite sowie die Schwäche des hiesigen Kapitalmarkts, die unter anderem zu Lücken in kritischen Kompetenzen führt. Zudem hat sich die schwache Kommunikations- und Kooperationskultur der Akteure untereinander als großes Manko des deutschen IT-Sicherheitsmarkts herausgestellt. Diese nimmt den Unternehmen zum einen Chancen bei Auslandsgeschäften, wo Kooperationen den größeren Erfolg bei Ausschreibungen versprechen. Die fragmentierte Anbie-

terstruktur erschwert zum anderen eine effiziente Unterstützung der Unternehmen durch den Staat im Ausland.

Die übergreifende und strukturelle Natur der erkannten Schwächen, die nicht das Agieren einzelner Marktteilnehmer, sondern die heimischen Unternehmen im Bereich der IT-Sicherheit insgesamt betreffen und aus ordnungs- wie wettbewerbspolitischer Sicht auch für den Standort Deutschland insgesamt von Relevanz sind, begründen ein ordnungspolitisches Handeln des Staates im Bereich der IT-Sicherheit. Insgesamt wurden 11 Handlungsfelder mit 36 Einzelmaßnahmen in den Handlungszielen „Sicherung kritischer Kompetenz", „Innovation" und „Wachstum" aus der Stärken und Schwächen Analyse erarbeitet.

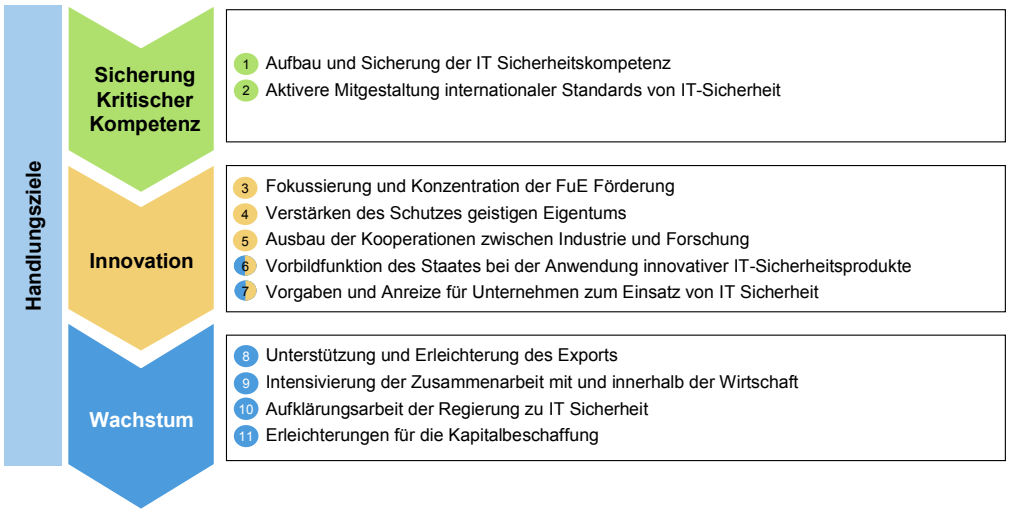


Abbildung 2: Übersicht der ordnungspolitischen Handlungsfelder

Der Maßnahmenkatalog wurde, entsprechend des Studienauftrags, weitgehend für die Perspektive und Aufgabenschwerpunkt des BMWi entwickelt. In vielen Punkten ist jedoch das Agieren mehrerer öffentlicher Akteure, darunter weitere Ressorts des Bundes, aber auch von Organisationen auf Landesebene usw. relevant. Insgesamt kommt die Studie zu dem Ergebnis, dass bei nachdrücklicher Umsetzung der Einzelmaßnahmen in den kommenden 36 Monaten der Staat wichtige Wachstumsimpulse für die IT-Sicherheitsbranche setzen und dazu beitragen kann, bis zum Jahr 2012 das Wachstum in Deutschland in dieser Branche von derzeit ca. 10% zumindest auf das Niveau des weltweiten Wachstums von ca. 14 Prozent zu heben.

Allerdings reichen die staatlichen Maßnahmen alleine nicht aus. Auch die Unternehmen sind, etwa bei der Verbesserung der Kommunikation und Koope-

ration untereinander, in der Pflicht und sollten die in diesen Maßnahmen enthaltenen Angebote konstruktiv annehmen und aktiv mit ausgestalten.

2 Aufgabenstellung der Studie

Das Bundesministerium für Wirtschaft und Technologie (BMWi) hat im Juli 2009 Booz & Company mit der Durchführung der Studie „Die IT-Sicherheitsbranche in Deutschland – Aktuelle Lage und ordnungspolitische Handlungsoptionen“ beauftragt.

2.1 Hintergrund und Zielsetzung der Studie

Das Thema IT-Sicherheit findet zunehmend Berücksichtigung in der öffentliche Diskussion. Nicht zuletzt öffentlich gewordene Vorfälle von Sicherheitsverletzungen im Bereich Datenschutz haben die Aufmerksamkeit für das Thema auch außerhalb der IT-Profession erhöht. Zugleich wird in Expertenkreisen eine intensive Diskussion um neue Bedrohungen im Bereich der IT-Sicherheit geführt. Neben intrinsisch motivierten Angriffen („klassische Hacker“) finden vermehrt wirtschaftlich motivierte Angriffe Beachtung. Peter Hinze, parlamentarischer Staatssekretär im Bundeswirtschaftsministerium, spricht von Computerkriminalität in „organisierter, ja industrialisierter Form“[2].

Darüber hinaus ist eine zunehmende Aktivität von ausländischen Regierungsstellen festzustellen, die mit gezielten Angriffen auf IT-Systeme eigene politische Interessen verfolgen bzw. Interessen der eigenen Wirtschaft fördern. Der wohl bekannteste Vorfall ereignete sich im Mai 2007, als sich Estland Internetangriffen aus Russland ausgesetzt sah. Die Bedeutung der Informationstechnologie und damit die Dimension eines potenziellen Schadens ist dabei inzwischen unermesslich. Bernhard Beus, der seinerzeitige Beauftragte der Bundesregierung für Informationstechnik, stellt hierzu fest: „Der Ausfall zentraler IT-Komponenten und der Verlust sensibler Informationen stellen in einem hoch technisierten Land wie Deutschland nicht bloß ein abstraktes Risiko dar, sondern eine tagtägliche Bedrohung.“[3]

IT-Sicherheit als Markt wiederum ist ein durchaus signifikanter Teil des gesamten Marktes für Informationstechnologie. Dennoch liegt für den deutschen Markt bisher noch keine aktuelle zusammenfassende Untersuchung aus

[2] Hinze, Peter: „Sicherheit 2009 Industrialisierung der Computerkriminalität“, 20.01 2009.

[3] Beus, Bernhard: „Strategische Industrie IT“ in griephan Global Security Ausgabe 1, 2009.

Standortperspektive vor. Existierende Studien wurden aus Unternehmens- / Absatzsicht verfasst und fokussieren somit auf die Nachfrageseite.

Wie generell im Bereich der Informationstechnologie und insbesondere Produktbereich (Hardware, Software) ist der Markt für IT-Sicherheit international. So dominieren in bestimmten Bereichen globale Anbieter den Markt länderübergreifend. Dies ist z.B. im Bereich der Firmen-Firewalls (z. B. Checkpoint) oder im Bereich Virenscanner (z. B. Symantec, McAfee, Kaspersky Lab) der Fall.

Die deutschen Anbieter im Bereich IT-Sicherheit werden als im internationalen Wettbewerb grundsätzlich gut aufgestellt gesehen. Allerdings fällt auf, dass in Deutschland, mit Ausnahme von T-Systems und Giesecke & Devrient hauptsächlich kleine spezialisierte Anbieter ansässig sind mit einem Umsatz von deutlich weniger als 100 Mio. Euro.

Aktuell wird die deutsche IT-Sicherheitsbranche durch eine Reihe von flankierenden ordnungspolitischen Maßnahmen gefördert. Relevante Initiativen sind z.B.:

- ITSMIG e.V.: IT-Sicherheit Made in Germany (BMWi, BMI)
- Netzwerk elektronischer Geschäftsverkehr - Netz- und Informationssicherheit (BMWi)
- Arbeitsprogramm IT-Sicherheitsforschung (BMI, BMBF)

Eine ganzheitliche Betrachtung der existierenden ordnungspolitischen Maßnahmen und eine Neubewertung vor dem Hintergrund der aktuellen Bedrohungs- und Wirtschaftslage liegt bisher jedoch noch nicht vor.

Vor diesem Hintergrund ist es Ziel dieser Studie, den Markt für IT-Sicherheit in Deutschland zu beleuchten. Dazu wird in einer Sektoranalyse die Marktgröße plausibilisiert, ein Überblick über die Anbieterseite gegeben und angesichts aktueller Markttrends eine Stärken- & Schwächen-Betrachtung vorgenommen. Auf dieser Basis werden schließlich ordnungspolitische Handlungsempfehlungen abgeleitet und ihre potenzielle Wirkung aufgezeigt.

2.2 Vorgehen und Aufbau der Studie

Die vorliegende Studie ist in fünf inhaltliche Module gegliedert, die den Abschnitten 3 bis 7 entsprechen.

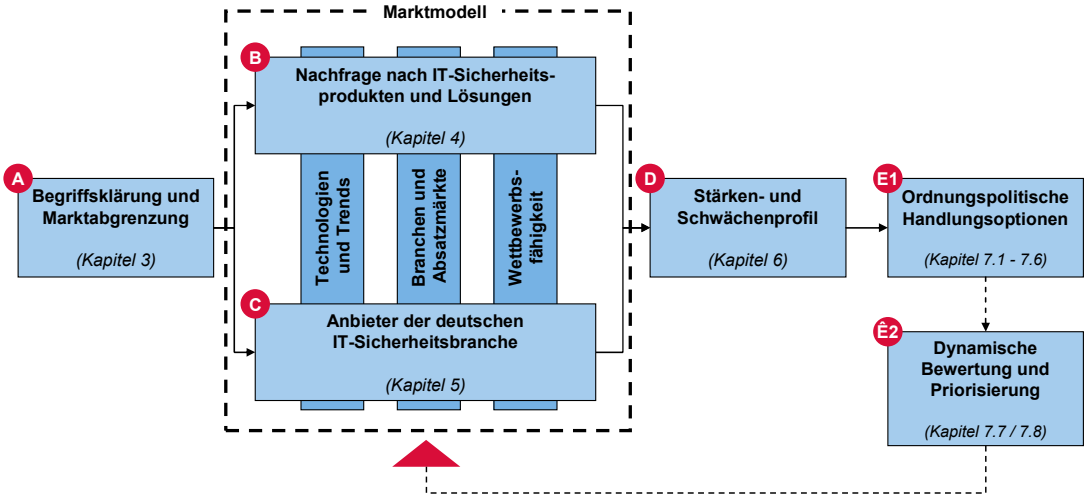


Abbildung 3: Aufbau der Studie

Im Abschnitt **3 Begriffsklärung und Marktabgrenzung** wird zunächst eine pragmatische Definition des Marktes für IT-Sicherheit im Rahmen dieser Studie entwickelt. Zielführend ist dabei die Marktstruktur zu spiegeln. Hiervon ausgehend wird eine Untersegmentierung des IT-Sicherheitsmarktes entlang der Anwendungsgebiete (z.B. Netzwerksicherheit) und Lebenszyklusphasen (z.B. Produktenwicklung, Betrieb von Lösungen etc.) erarbeitet.

Der Abschnitt **4 Nachfrage nach IT-Sicherheitsprodukten und Lösungen** beschreibt die aktuelle Nachfrage bzw. die erwarteten Entwicklungen im Markt. Die Marktgröße in Deutschland wird durch

- Analyse der Primärstudien zum IT-Markt für Deutschland und
- Analyse weltweiter bzw. europäischer Marktstudien zur IT-Sicherheit

plausibilisiert. Im zweiten Schritt werden die relevanten Treiber der Nachfrage analysiert. Diese lassen sich in folgende Kategorien einteilen:

- Aktuelle Entwicklungen der Bedrohungslage
- Neuartige Technologien, die neuartige Schutzkonzepte erfordern
- Wirtschaftliche und rechtliche Trends

Die Validierung der Erkenntnisse erfolgt durch ein Interviewprogramm mit Unternehmen auf der Nachfrageseite. Abschließend wird die künftige Nachfragenwicklung in den einzelnen Marktsegmenten abgeleitet, sowie relevante Wettbewerbsfaktoren herausgestellt.

Das Kapitel **5 Anbieter der deutschen IT-Sicherheitsbranche** komplettiert das Marktmodell durch die Betrachtung der Angebotsseite. Neben der Untersuchung der relevanten aktuellen Ereignisse und Trends auf Anbieterseite werden die wichtigsten deutschen sowie ausgewählte globale Anbieter im Profil dargestellt. Hierzu wurden eine Reihe strukturierter Interviews mit den betroffenen Unternehmen durchgeführt. Schwerpunkt der Darstellung ist insbesondere die Positionierung der deutschen Unternehmen gegenüber der internationalen Konkurrenz auf dem deutschen und internationalen Markt. Hieraus werden erste Anhaltspunkte für ordnungspolitische Handlungsnotwendigkeiten aus Sicht der Anbieter abgeleitet.

Die Erkenntnisse aus der Betrachtung von Nachfrage und Angebot werden im Abschnitt **6 Stärken- und Schwächenprofil** zusammengeführt. Auf Basis der Positionierung der deutschen Anbieter in den einzelnen Marktsegmenten wird ein Stärken- und Schwächenprofil der deutschen IT-Sicherheitswirtschaft erarbeitet. Mit Blick auf künftige Entwicklungen werden Chancen und Risiken für die deutschen Anbieter dargestellt.

Um in Abschnitt **7 die Ordnungspolitischen Handlungsoptionen** abzuleiten wird zunächst die aktuelle Regulierungslage und existierende Initiativen in Deutschland untersucht und der Situation in ausgewählten Ländern gegenübergestellt. Auf dieser Basis wird ein Katalog möglicher Handlungsoptionen dargestellt und priorisiert. Zudem werden die **Auswirkungen der Maßnahmen** auf das Marktmodell qualitativ bewertet.

3 Begriffsklärung und Abgrenzung des Marktes

3.1 Definition von IT-Sicherheit im Untersuchungsinteresse der Studie

Zunächst ist eine genaue Definition des Marktes für IT-Sicherheit notwendig, die dann als Basis für eine Quantifizierung des Marktes sowie zur Auswahl der zu betrachtenden Anbieter dienen kann. Im Bereich der IT-Sicherheit werden in der Regel zwei Begriffe unterschieden:

- Der Begriff **Informationssicherheit** bezeichnet die Sicherstellung von Vertraulichkeit, Verfügbarkeit und Integrität von Informationen innerhalb und außerhalb von IT-Systemen. Der Begriff umfasst also auch Informationen, die z. B. auf Papier oder „in den Köpfen" von Mitarbeiten vorhanden sind.
- Der Begriff **IT-Sicherheit** bezieht sich in der Regel auf die Vertraulichkeit, Verfügbarkeit und Integrität von Daten in IT-Systemen (Security for IT).

Im Untersuchungsinteresse dieser Studie ist weniger eine wissenschaftliche als vielmehr eine pragmatische Definition in Hinblick auf die Einordnung der Anbieter und die Ableitung von Handlungsoptionen sinnvoll:

- Möglichst **eindeutige Zuordnung von Produkten und Anbietern**: Die Definition sollte so erfolgen, dass die Produkte im Umfeld der IT-Sicherheit eindeutig als innerhalb bzw. außerhalb des Marktes zuordenbar sind. Idealerweise sind auch die Anbieter mit ihrem gesamten Angebotsspektrum dem Marktsegment zuordenbar. Bei größeren Konzernen gilt dies entsprechend für die Geschäftseinheiten.
- Möglichst klare **Abgrenzung der Nachfrage**: Die Definition sollte anhand der relevanten Organisationseinheiten bzw. Budgetumfänge der nachfragenden Unternehmen erfolgen.

Um zu einem derart handhabbaren Begriff von (IT-)Sicherheit im engeren Sinn zu gelangen, ist diese von der bloßen Funktions- und Betriebssicherheit abzugrenzen. Denn anders als im englischen Sprachgebrauch, der zwischen „security" einerseits und „safety" andererseits unterscheidet, umfasst das deutsche Wort „Sicherheit" grundsätzlich beides. Die bloße Funktions- und Betriebssicherheit z. B. im Sinne physischer Schutzmaßnahmen für IT-Systeme soll jedoch nicht Gegenstand dieser Untersuchung sein.

Aus Sicht der Nachfrage bzw. des Bedarfs an IT-Sicherheit ist zunächst die Art der Information zu unterscheiden, die geschützt werden soll. Im Rahmen dieser Studie wird der Schutz von Informationen außerhalb von IT-Systemen nicht als Bestandteil des Marktes für IT-Sicherheit angesehen. Dies entspricht auch dem allgemeinen Begriffsverständnis von IT-Sicherheit (vgl. auch Abbildung 4).

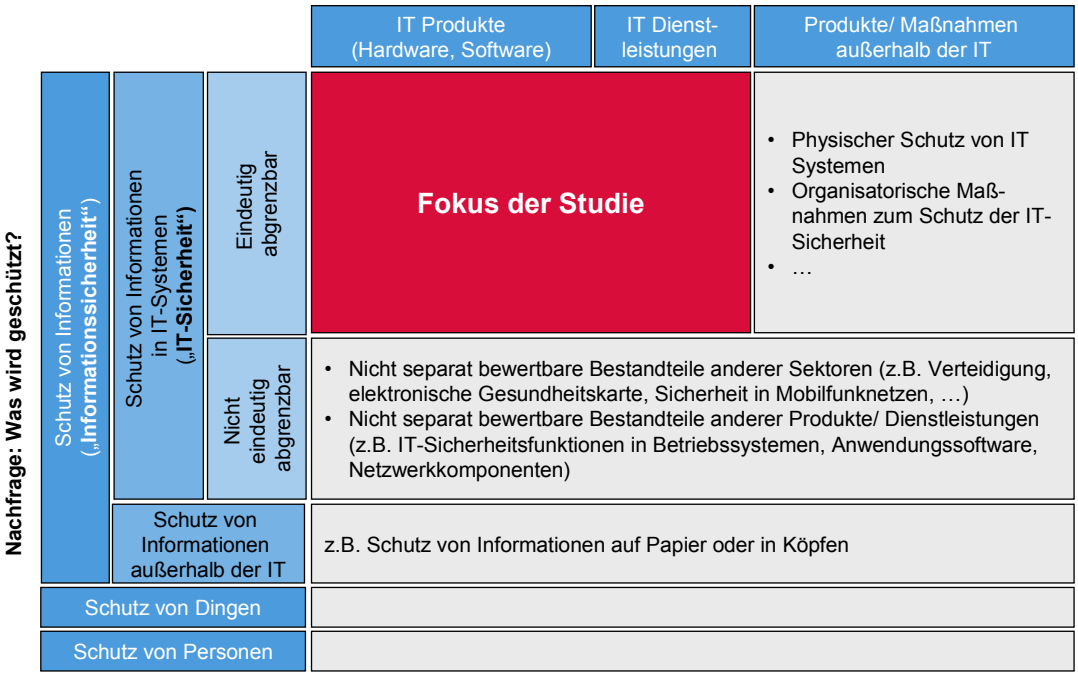


Abbildung 4: Eingrenzung des Markts für IT-Sicherheit

Aus Gründen der Abgrenzbarkeit wird auch der Schutz von Informationen in folgenden Bereichen nicht als Bestandteil dieses Marktes angesehen:

- **Nicht separat bewertbare Bestandteile anderer Sektoren** (z. B. Schutz der Telekommunikationsinfrastruktur, nicht separierbare Schutzmechanismen von Endgeräten der Telekommunikation, spezielle Schutzbedürfnisse im Bereich der Landesverteidigung usw.)
- **Nicht separat bewertbare Bestandteile anderer Produkte** (z. B. integrierte Sicherungsmechanismen in ERP-Systemen, Verschlüsselungsfunktionen in Web-Browsern und Web-Servern usw.). Exakt definierbare Komponenten, die als hinzugekaufte Vorleistung in diese Produkte einfließen sind allerdings Bestandteil des Betrachtungsumfangs.
- **Produkte und Dienstleistungen im Bereich der Verfügbarkeit von IT-Systemen**, soweit sie nicht auf die Abwehr konkreter Bedrohungen zielen,

sondern Redundanzen bereitstellen oder die Datenspeicherung betreffen (z. B. Back-up-Systeme und -software, unterbrechungsfreie Stromversorgung, redundante Auslegung von Rechenzentren, Servern und einzelner Komponenten usw.)

Was die Angebotseite betrifft, also die Produkte und Dienstleistungen, mit denen der Schutzbedarf gedeckt wird, sind Produkte und Dienstleistungen der Informationstechnologie Bestandteil des in dieser Studie dargestellten Marktes. Insbesondere sind dies:

- **Software** zum Einsatz auf Servern, Netzwerkkomponenten und Endgeräten
- Dedizierte **Hardware** zum Schutz von IT-Systemen bzw. vorkonfigurierte Kombinationen von Hard- und Software (sog. Appliances)
- **Dienstleistungen**, die speziell auf den Schutz von IT-Systemen abzielen bzw. in direktem Zusammenhang mit der Entwicklung, der Implementierung, dem Betrieb und dem Management entsprechender Hard- und Software stehen (vgl. auch Abschnitt 3.4).

Nicht im Betrachtungsumfang der Studie liegen demzufolge grundsätzliche organisatorische Maßnahmen zum Schutz der IT-Systeme (z. B. Personenkontrollen oder Sicherheitsrichtlinien, die nicht allein auf IT-Systeme abzielen) und physische Maßnahmen (z. B. baulicher Schutz von Rechenzentren).

Zusammenfassend lässt sich der betrachtete Markt wie folgt beschreiben:

*Der „**Markt für IT Sicherheit**“ umfasst IT-Produkte und IT-Dienstleistungen zum Schutz der Informationstechnologie in Unternehmen, in der öffentlichen Verwaltung und in Privathaushalten (**„security for IT“**), sofern sie nicht untrennbarer Bestandteil anderer Produkte, Dienstleistungen oder Sektoren sind.*

3.2 Abgrenzung „deutsche Anbieter“

Neben der Definition des relevanten Marktes ist die Eingrenzung der im Rahmen der Studie betrachteten Anbieter notwendig. Grundsätzlich soll die Untersuchung auf „deutsche Anbieter“ fokussiert werden. Eine Eingrenzung dieser Anbietergruppe ist in zwei Dimensionen möglich (siehe Abbildung 5): Zum einen kann auf die **Eigentümerstruktur** abgestellt werden, zum anderen auf den **Wertschöpfungsanteil in Deutschland**.

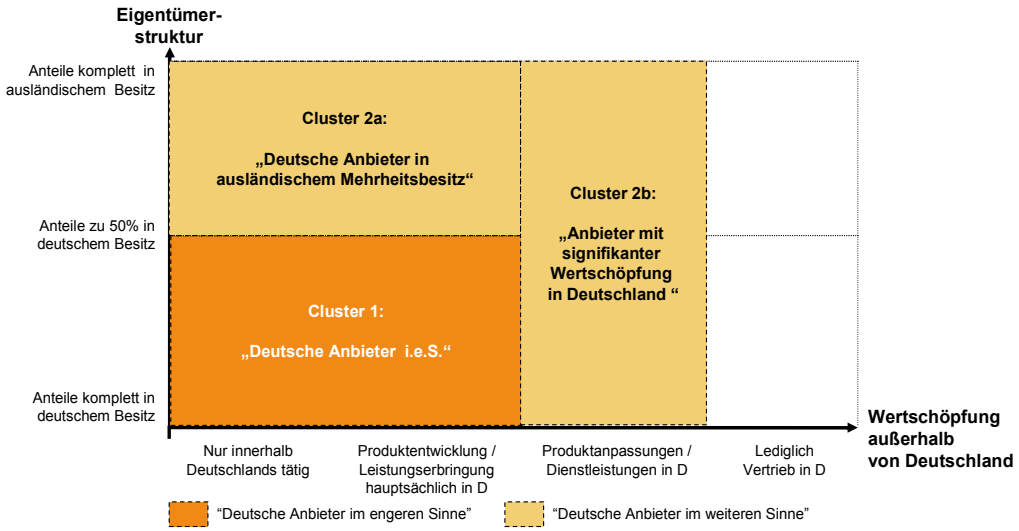


Abbildung 5: Abgrenzung "deutscher Anbieter"

In Bezug auf die **Eigentümerstruktur** und damit hinsichtlich der tatsächlichen Verfügungsgewalt über die Unternehmensanteile sind zunächst Anbieter zu betrachten, die sich mehrheitlich im Besitz von anderen deutschen Unternehmen, der öffentlichen Hand oder deutschen Privatpersonen befinden. Ihnen stehen diejenigen Unternehmen gegenüber, die nicht oder nur über eine Minderheitsbeteiligung in deutschem Besitz sind. Relevant ist diese Einteilung für die Analyse der Auswirkungen von ordnungspolitischen Maßnahmen: Einerseits können so deren Auswirkungen auf deutsche oder ausländische Firmen, Privatpersonen oder staatliche Stellen abgeleitet werden. Auf der anderen Seite können im Falle eines überwiegend deutschen Eigentums staatliche Interessen (z. B. Zugriff auf Kryptokompetenz, Geheimschutzverpflichtungen, Veräußerungsauflagen) leichter durchgesetzt werden. Alterna-

tiv hierzu ist eine Absicherung über individuelle rechtliche Regelungen denkbar.

Um die Auswirkungen staatlicher Maßnahmen auf das Wirtschaftsgeschehen in Deutschland und die Arbeitsplätze in Deutschland einzuschätzen, ist eine Unterscheidung nach dem Grad der in Deutschland erbrachten Wertschöpfung nötig. Das Spektrum reicht hierbei von

- Firmen, die **nur innerhalb von Deutschland tätig** sind, über
- Anbieter, bei denen **der Hauptteil der Leistungserbringung bzw. der Produktentwicklung in Deutschland** stattfindet, und über
- Anbieter die **in Deutschland lediglich Produktanpassungen** („Customizing") vornehmen und **Dienstleistungen** erbringen, bis hin zu
- Firmen, die in Deutschland **lediglich vertrieblich** (ggf. nur über Vertriebspartner) tätig sind.

Da beide Dimensionen für das Betrachtungsumfeld der Studie relevant sind, werden nachfolgend zwei Cluster unterschieden:

Cluster 1: „Deutsche Anbieter im engeren Sinne" sind Anbieter, die sowohl mehrheitlich in deutschem Besitz sind als auch den Hauptteil der Wertschöpfung in Deutschland erbringen (vgl. Abbildung 5).

Cluster 2: „Deutsche Anbieter im weiteren Sinne" sind Firmen, die nicht dem Cluster 1 angehören, aber einen signifikanten Anteil ihrer Wertschöpfung in Deutschland erbringen.

Beide Cluster finden in der Praxis Anwendung. So können im Verein „IT Security made in Germany (ITSMIG e.V.)" nur Firmen aus dem Cluster 1 Mitglied werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) legt den Fokus hingegen mehr auf den Anteil der Wertschöpfung, insbesondere im Hochsicherheitsbereich, da dieser Aspekt bei Zertifizierungen bzw. Zulassungen eine wesentliche Rolle spielt.

In den weiteren Ausführungen dieser Studie werden beide Gruppen betrachtet, jedoch mit einem besonderen Fokus auf Cluster 1 „Deutsche Anbieter i. e. S.".

3.3 Taxonomie der für das Untersuchungsinteresse der Studie relevanten Produkte und Dienstleistungen

Neben der eindeutigen Abgrenzung des zu betrachtenden Marktes ist eine Segmentierung in Teilbereiche notwendig, um zutreffende und detaillierte Aussagen zu Marktentwicklung, Anbietersituation und Handlungsoptionen zu treffen. Nachfolgend soll eine Taxonomie vorgestellt werden, die den Markt für IT-Sicherheit in zwei weitere Ebenen aufgliedert (siehe Abbildung 6).

	Marktsegment 1. Ebene	Marktuntersegment 2. Ebene
Produkte	Netzwerksicherheit	Firewall
		Intrusion Detection & Prevention
		Virtual Private Network
		Network Access Control
		Wireless Security
	Endgerätesicherheit	Personal Firewall
		Antivirus, Malware
		Application/ Device Control
		Mobile Devices
	Nachrichtensicherheit	Messaging Server Security
		Messaging Client Security
	Websicherheit	Web-Browser Security
		Web-Server Security
	Applikationssicherheit	Application and Code Testing
		Application Integrity
		Security Toolkits
	Datensicherheit	Encryption
		Data Loss Prevention
		Digital Rights Management
		Crypto-Accelerators
	Identitäts- und Zugriffsverwaltung	User/ Authorization Management
		Strong Authentication
		Smartcards
		PKI and Key Management
Dienstleistungen	Dienstleistungen (unabhängig von Produkten)	Security Assessments
		Security Strategy & Architectures
		Training, Awareness
		Log & Configuration Management
		Forensic / Incident Investigation
		Certification

Abbildung 6: Taxonomie des Marktes für IT-Sicherheit[4]

[4] Zur Beschreibung der 2. Ebene innerhalb der Martktsegmentierung wurde auf englischsprachige Begriffe zurückgegriffen, da entsprechende deutsche Begrifflichkeiten nicht existieren oder kaum verbreitet sind.

Die Segmentierung des Marktes erfolgt hierbei anhand der Anwendungsgebiete bzw. der Schutzobjekte. Dienstleistungen, die im direkten Zusammenhang mit den Anwendungsgebieten stehen, sind diesen zugeordnet. Übergreifende Dienstleistungen, wie z. B. Sicherheitsprüfungen oder die Erstellung von Sicherheitsstrategien und –architekturen, werden getrennt aufgeführt.

Die Hauptanwendungsgebiete im Bereich Produkte sind die Sicherheit von Netzwerken, Endgeräten, Applikationen und Daten, ergänzt um den Bereich Identitäts- und Zugriffsverwaltung.

3.3.1 Netzwerksicherheit

Der Bereich Netzwerksicherheit befasst sich mit der Sicherheit von internen und externen Netzwerken insbesondere gegen Bedrohungen von außerhalb des betreffenden Netzwerksegments.

Tabelle 2: Unterteilung des Marktsegments Netzwerksicherheit

Untersegment (2. Ebene)	Beschreibung
Firewall	Systeme zur Abschottung von Netzwerksegmenten auf der Basis von Software oder Hardwarekomponenten. In der Regel wird unterschieden zwischen reinen Paketfiltern und Firewall-System, die den Datenverkehr auch auf der Applikationsebene untersuchen. Personal Firewalls, die lediglich ein Endgerät (z. B. einen Arbeitsplatzrechner) schützen, fallen nicht in dieses Segment, sondern sind dem Untersegment Personal Firewall (Segment Endgerätesicherheit) zugeordnet.
Intrusion Detection & Prevention	Software und Hardware mit der Funktion, unerwünschte Zugriffe, Manipulationen, Angriffe bzw. entsprechende Versuche aufzudecken und ggf. zu verhindern.
Virtual Private Network (VPN)	Software und Hardware, die eine sichere Kommunikation zwischen zwei Netzen bzw. Endgeräten über ein unsicheres öffentliches Netz gewährleistet. In der Regel erfolgt der Datenaustausch verschlüsselt. Die Authentifizierung der Benutzer kann durch ein einfaches Passwort, aber auch durch zusätzliche Hardware erfolgen (z. B. PIN-Generator).
Network Access Control	Software und Hardware, die das Ankoppeln von unerwünschten, nicht zugelassenen Endgeräten an Netzwerke beschränkt.

Wireless Security	Technologien zum Schutz spezieller drahtloser Netzwerke wie z. B. Wireless LAN.

3.3.2 Endgerätesicherheit

Unter Endgerätesicherheit wird der Schutz vor ungewollten Eingriffen am Endgerät selbst verstanden.

Tabelle 3: Unterteilung des Marktsegments Endgerätesicherheit

Untersegment (2. Ebene)	Beschreibung
Personal Firewall	Software, die den ein- und ausgehenden Datenverkehr eines PCs auf dem Rechner selbst filtert. Im Gegensatz zu einer klassischen Netzwerk-Firewall filtert die Personal Firewall nicht den Verkehr zwischen zwei Netzwerken, sondern überprüft nur die Kommunikation zwischen dem PC, auf dem sie betrieben wird, und dem Netz.
Antivirus und Malware	Software, die bekannte Computerviren oder Schadprogramme (Sammelbegriff für Programme, die entwickelt wurden, um vom Benutzer nicht erwünschte und ggf. schädliche Funktionen auszuführen) aufspürt, meldet, blockiert und gegebenenfalls beseitigt.
Application/ Device Control	Programme zum Erkennen und Sperren nicht zugelassener Wechseldatenträger, optischer Medienlaufwerke und Drahtlosprotokolle (z. B. WiFi, Bluetooth und Infrarot) sowie Programme zum Sperren einzelner Applikationen, Typen von Applikationen oder Technologien.
Mobile Devices	Programme, die speziell mobile Endgeräte vor ungewollten Fremdeingriffen schützen (z. B. Mobile Antivirus, Mobile Antispyware).

3.3.3 Nachrichtensicherheit

Unter Nachrichtensicherheit wird der Schutz des Austausches elektronischer Nachrichten (insbesondere E-Mail) verstanden.

Tabelle 4: Unterteilung des Marktsegments Nachrichtensicherheit

Untersegment (2. Ebene)	Beschreibung
Messaging Server Security	Produkte und Lösungen, die im Zusammenhang mit der Sicherung von Nachrichtenservern (insbesondere E-Mail-Server) stehen. Hierunter fallen z. B. die serverseitige E-Mail-Filterung zur Spamvermeidung, Server-Virenscanner, Inhaltsfilter und Kontrollprodukte zur Überwachung des E-Mail-Verkehrs.
Messaging Client Security	Produkte und Lösungen zur clientseitigen Sicherung des Nachrichtenaustausches, insbesondere clientbasierte Spam-Filter oder Inhaltsfilter. Virenscanner, die sowohl das Dateisystem als auch den E-Mail-Verkehr überprüfen, fallen unter die Kategorie Endgerätesicherheit. Funktionen zur Verschlüsselung des E-Mail-Verkehrs sind oft in Kryptographielösungen integriert.

3.3.4 Web-Sicherheit

Der Begriff Web-Sicherheit fasst alle Produkte zusammen, die der sicheren Nutzung des World Wide Web dienen.

Tabelle 5: Unterteilung des Marktsegments Web-Sicherheit

Untersegment (2. Ebene)	Beschreibung
Web-Server Security	Sicherheitsprodukte und Lösungen, welche die Internetnutzung serverseitig schützen. Dazu gehören z. B. Web-Filter-rodukte und Lösungen zur Härtung von E-Mail-Servern.
Web-Browser Security	Produkte, welche die Sicherheit des Web-Browsers erhöhen. Darunter fallen z. B. Pop-up-Blocker, Software zum Schutz vor Sicherheitsbedrohungen durch Web-Sites wie Phishing (Versuch, über gefälschte Web-Adressen an persönliche Daten zu gelangen) und Programme zum Schutz vor Adware (unerwünschte Werbeprogramme) oder Dialern.

3.3.5 Applikationssicherheit

Neben dem Schutz von Netzwerken und Endgeräten sind die Applikationen selbst gegen unbefugten Zugriff, Angriffe und Fehlverhalten bzw. Umgebungsversagen zu schützen.

Tabelle 6: Unterteilung des Marktsegments Applikationssicherheit

Untersegment (2. Ebene)	Beschreibung
Application and Code Testing	Untersuchung der Applikation bzw. ihres Quellcodes auf eventuelle Schwachstellen und Sicherheitsrisiken. Neben entsprechenden automatisierten Werkzeugen wird dies insbesondere als Dienstleistung angeboten.
Application Integrity	Mechanismen zum Schutz von Softwareprodukten gegen Manipulationen durch Anwender bzw. Dritte. Dies erfolgt in der Regel durch eine elektronische Signatur der Programmdateien, die durch ein Zertifikat des Softwareanbieters oder bei einer Zertifizierungsinstanz überprüft wird (z. B. Signatur von Treibern für den Einsatz in MS Windows, Signatur von Java Applets für die Verteilung über das Internet).
Security Toolkits	Softwarebibliotheken, die dazu dienen, innerhalb von Softwareprodukten wiederum Sicherheitsfunktionen (z. B. Verschlüsselung, elektronische Signatur) zu nutzen.

3.3.6 Datensicherheit

Die IT-Datensicherheit umfasst alle Maßnahmen zur Wahrung der Vertraulichkeit, Verfügbarkeit, Integrität und Originalität von Daten.

Tabelle 7: Unterteilung des Marktsegments Datensicherheit

Untersegment (2. Ebene)	Beschreibung
Encryption	Verfahren zur Umwandlung von Daten derart, dass diese mithilfe eines Algorithmus verschlüsselt werden. Danach können sie nur noch über den Encryption-Key gelesen werden.
Data Loss Prevention	Verfahren, welches den Schutz der Vertraulichkeit und Integrität von Daten unterstützt. Dabei geht es sowohl um die Verhinderung der Entwendung von Daten über USB-Sticks und Wechseldatenträger als auch um den Datentransfer über E-Mail oder Datei-Uploads.
Digital Rights Management	Verfahren, mit dem die Nutzung (und Verbreitung) digitaler Medien kontrolliert wird. Dieses gibt dem Rechteinhaber von Informationsgütern die Möglichkeit, die Art der Nutzung seines Eigentums auf Basis einer zuvor getroffenen Nutzungsvereinbarung technisch zu überwachen.
Crypto-accelerators	Hardware-Produkte zur Beschleunigung des Ver- und Entschlüsselungsverfahrens. Sie sind relevant insbesondere bei massenhaften Ver- und Entschlüsselungvorgängen, wie sie z. B. bei der Verwendung des HTTPS-Protokolls auf stark frequentierten Web-Servern vorkommen. Gleiches gilt für Massensignatur-Erfordernisse (z.B. automatisierte Rechnungssignatur).

3.3.7 Identitäts- und Zugriffsverwaltung

Unter Identitäts- und Zugriffsverwaltung wird die zentrale Verwaltung digitaler Identitäten und deren Rechte inklusive aller unterstützenden Soft- und Hardware verstanden.

Tabelle 8: Unterteilung des Marktsegments Identitäts- und Zugriffsverwaltung

Untersegment (2. Ebene)	Beschreibung
User / Authorization Management	Systematische Organisation der Identifikation von Nutzern eines Systems (Angestellte, Kunden, Vertragspartner etc.) und die Regelung des Zugangs zu dessen Ressourcen.
Strong Authentication	Autorisierungsprozess, bei dem mehrere Faktoren in Kombination verwendet werden. Dabei wird meist eine Login-Passwortidentifikation mit einer physischen Autorisierung verbunden (z. B. Smartcard, Biometrie, Passwort-Generator). Dadurch wird eine höhere Sicherheit gewährleistet.
Smartcards	Smartcards werden als sichere Informations- oder Schlüsselspeicher genutzt, die gleichzeitig auch verschiedene Sicherheitsdienste wie Authentifying, Verschlüsselung und Signatur darstellen können. Da die kryptographischen Funktionen auf der Karte selbst ausgeführt werden, ist es nicht nötig (und auch nicht möglich), private Schlüssel von der Karte abzuleiten, was den Schutz der Schlüssel ganz erheblich verbessert.
PKI and Key Management	Infrastruktur, welche die Absicherung einer computergestützten Kommunikation ermöglicht. Erreicht wird dies dadurch, dass digitale „Zertifikate“ zugeordnet werden, welche die Identität der Teilnehmer sicherstellen.

3.3.8 Dienstleistungen

Unter IT-Sicherheitsdienstleitungen werden sämtliche Dienstleistungen verstanden, die im Zusammenhang mit der IT-Sicherheit stehen, aber unabhängig von den Produkten sind.

Tabelle 9: Unterteilung des Marktsegments Dienstleistungen

Untersegment (2. Ebene)	Beschreibung
Security Assessments	Bewertung der Sicherheit der IT-Infrastruktur (auf Projektbasis oder kontinuierlich). Bei einer kontinuierlichen Sicherheitsüberprüfung wird diese automatisch in regelmäßigen Abständen und bei jeder Änderung der Firewall-Policy durchgeführt, sodass dass das Unternehmen zeitnah über den aktuellen Sicherheitszustand der externen Zugänge informiert ist. In vielen Unternehmen wird sie gegen eine feste Jahresgebühr von einer externen Firma gelistet .
Security Strategy & Architectures	Entwicklung eines umfassenden Ansatzes für IT-Sicherheit, der die Beschreibung der Struktur, der Prozesse, des IT-Systems selbst und der dafür notwendigen Organisation (inkl. Personal) leistet. Ziel ist es, das IT-Sicherheitssystem an der Struktur, der Strategie und der Sicherheitsphilosophie des Unternehmens auszurichten.
Training, Awareness	Trainingsmaßnahmen hinsichtlich der Handhabung spezifischer Systeme sowie der Förderung des allgemeinen Sicherheitsbewusstseins im Unternehmen.
Log & Configurations Management	Erhebung, Zusammenführung und Analyse von Log-Dateien (Dateien, die Informationen über konkrete Vorgänge in IT-Systemen speichern) sowie Ableitung entsprechender Maßnahmen.
Forensic / Incident Investigation	Untersuchung IT-sicherheitsrelevanter Vorgänge sowie ihrer Auswirkungen, z. B. zur Quantifizierung von Schadensersatzforderungen und zurVorbereitung möglicher Gerichtsverfahren.
Certification	Überprüfung und Bestätigung bestimmter Charakteristika von IT- Sicherheitsprodukten und -systemen. Die Prüfung von Prozessen unter Compliance-Gesichtspunkten (z.B. durch Wirtschaftsprüfer) fällt nicht hierunter.

3.4 Gesamtzyklussicht IT-Sicherheit

Neben der Einteilung nach Anwendungsgebieten nehmen die Akteure im Markt für IT-Sicherheit (wie in der Informationstechnologie im Allgemeinen) verschiedene Stellungen im Produktlebenszyklus ein. Dieser beschreibt den Weg von Innovationen in der Grundlagenforschung über die Produktentwicklung, Herstellung, Konzeption, Implementierung und den Betrieb bis hin zum kompletten Outsourcing bzw. Fremdmanagement (vgl.

Abbildung 7).

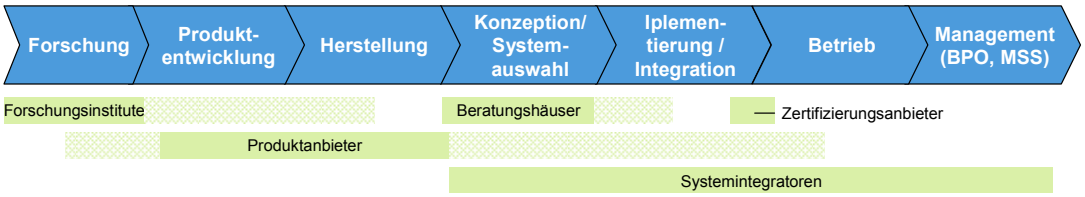


Abbildung 7: Gesamtzyklussicht auf IT-Produkte und -Dienstleistungen

3.4.1 Forschung

Auch wenn die IT-Sicherheitsforschung und insbesondere die Grundlagenforschung nicht direkt als ein Teil des Marktes für IT-Sicherheitsleistungen angesehen werden kann, bildet sie doch eine Basis für die Produktentwicklung in den Unternehmen. Darüber hinaus verschwimmen im Rahmen von Forschungspartnerschaften und Technologieclustern die Grenzen zwischen Forschung und Produktentwicklung.

3.4.2 Produktentwicklung

Im IT-Bereich ist generell der Anteil der Produktentwicklung an der Wertschöpfung innerhalb des Gesamtzyklus vergleichsweise hoch. Dies trifft insbesondere für den Softwarebereich zu: Hier sind die Reproduktions- bzw. Herstellungskosten fast zu vernachlässigen. Mit anderen Worten: Hier fallen fast die gesamten mit dem Produkt verbundenen Kosten in der Entwicklungsphase an. Ebenso Bestandteil dieser Phase ist die Entwicklung und Bereitstellung von Produktaktualisierungen, z.B. regelmäßige Aktualisierung der Definitionsdateien bei Virenscannern.

3.4.3 Herstellung

Die Herstellung von Softwareprodukten ist, wie erwähnt, nur mit geringen zusätzlichen Kosten (u. a. für Datenträger) verbunden. Daher ist die Herstellungsphase hauptsächlich für IT-Hardwareprodukte relevant.

3.4.4 Konzeption/Systemauswahl

Da die Anforderungen der Unternehmen sehr spezifisch sein können und die Gewährleistung einer optimalen Sicherheit nur durch ein individuell abgestimmtes Konzept bzw. System erfolgen kann, werden in dieser Phase oft externe Beratungsleistungen in Anspruch genommen. Dabei ist sowohl die Auswahl des Anbieters bzw. Produkts als auch die Konzeption der zu implementierenden Lösung von Bedeutung.

3.4.5 Implementierung/Integration

Um eine größtmögliche Sicherheit zu gewährleisten und gleichzeitig einen effizienten Betrieb zu ermöglichen, muss das IT-Sicherheitssystem meist spezifiziert und in die Organisation und Prozesse der IT-Infrastruktur integriert werden. Oft erfolgt dies durch den Anbieter des Systems, da dieser die Implementierung und Integration in Verbindung mit dem Produkt verkauft.

3.4.6 Betrieb

Der Betrieb von Software- und Hardwarekomponenten der IT-Sicherheit innerhalb des Unternehmens durch einen Drittanbieter umfasst insbesondere die Wartung, die Aktualisierung, die Fehlerbehebung und die Systemüberwachung. Die Gewährleistung des Betriebs durch Dritte ist u. a. vor dem Hintergrund der Wartungsintensität der Systeme sowie dem hohen Interesse an einem störungsfreien Ablauf relevant. Dabei ist der Übergang zwischen dem Betrieb und dem Management des IT- Sicherheitssystems in manchen Bereichen fließend.

3.4.7 Management (BPO, MSS)

Unter dem Management von IT-Sicherheitssystemen (auch als Managed Security Services bezeichnet) wird im Unterschied zum reinen Betrieb primär die kontinuierliche Konfiguration der Systeme wie zum Beispiel das Einspielen von neuen Software-Versionen und die aktive Überwachung und Analyse sowie die Einleitung von Gegenmaßnahmen verstanden. Angeboten wird z. B. das Management von Routern, Firewalls und Virenschutz-Gateways.

Darüber hinaus fällt auch die komplette organisatorische Auslagerung des Sicherheitssystems zu den Management Services. Im Extremfall wird die entsprechende Hardware auch physisch separiert betrieben und der komplette Prozess IT-Sicherheit ausgelagert.

3.5 Kompetenzraster für IT Sicherheit

Durch die Kombination der Taxonomie relevanter Produkte mit der Gesamtzyklussicht kann ein Raster erzeugt werden, das eine Einordnung der IT-Sicherheitsanbieter in Abschnitt 5 ermöglicht. Wie schon in den jeweiligen vorherigen Abschnitten ausgeführt, werden dabei dem Dienstleistungssegment nur die produktunabhängigen Dienstleistungen zugeordnet.

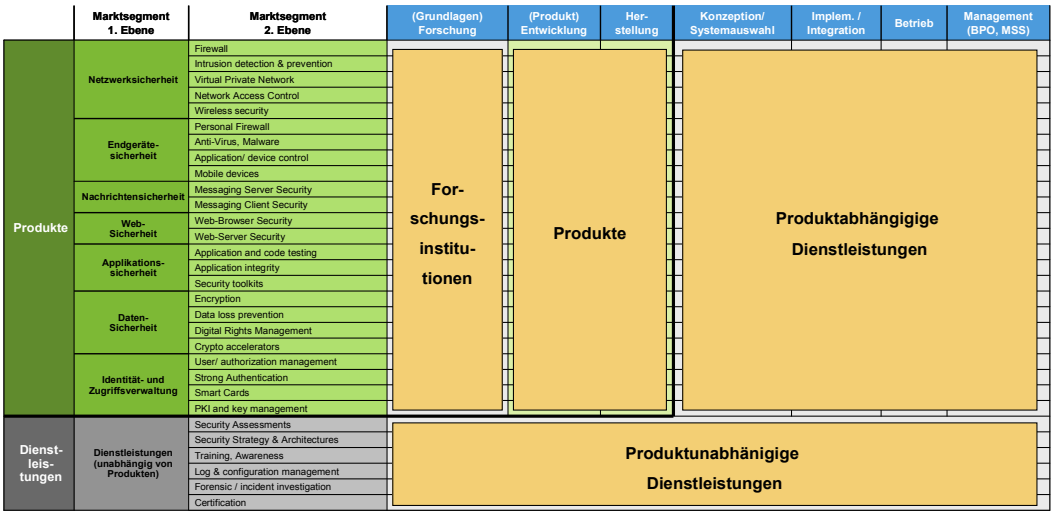


Abbildung 8: Kompetenzraster für IT-Sicherheit

4 Nachfrage nach IT-Sicherheitsprodukten und -lösungen

Der Markt für IT-Sicherheitsprodukte und –lösungen teilt sich auf der Nachfrageseite in die drei Segmente Privatwirtschaft, öffentliche Hand und Privathaushalte auf (Abschnitt 4.1). Während die Analysten insgesamt für die letzten Jahre ein signifikantes Wachtum ausweisen, gehen die Abschätzungen zu konkreten Umsatzzahlen (u. a. bedingt durch unterschiedliche Erhebungsmethodiken) weit auseinander (Abschnitt 4.2). Ein wichtiger Einflussfaktor für das Umsatzwachstum sind die Entwicklungen in der IT-Bedrohungslage (Abschnitt 4.3), welche im Blick auf Schwachstellen von IT-Systemen (Abschnitt 4.3.1), auf Bedrohungsszenarien in bestimmten Technologien (Abschnitt 4.3.2) und auf Bedrohungen im Bereich der kritischen Infrastruktur (Abschnitt 4.3.3) betrachtet werden können. Potenzielle neue Bedrohungen sowie Kosten- und Effizienzüberlegungen bilden den Hintergrund für die aktuellen Trends auf der Nachfrageseite (Abschnitt 4.4) und die Attraktivität der einzelnen Marktsegmente (Abschnitt 4.5). Neben einzelnen Segmenten haben auch bestimmte Regionen ein besonderes Wachstumspotenzial (Abschnitt 4.6). Um in diesen Märkten in Zukunft erfolgreich zu sein, müssen die Anbieter von IT-Sicherheit die relevanten Wettbewerbsfaktoren (Abschnitt 4.7) berücksichtigen.

4.1 Darstellung der Nachfrageseite

Der Schutz von IT-Infrastrukturen, Informationen und Wissen gewinnt branchenübergreifend weiter an Bedeutung: Über alle Industrien hinweg planen nach Forrester-Umfragen über 30% der Unternehmen eine Erhöhung des IT-Sicherheitsbudgets. Dabei wird der Anteil der IT-Sicherheit am IT-Gesamtbudget auf ca. 10% beziffert.[5] Grundlage für diesen allgemeinen Trend ist u. a. das Bestreben, Informationen und Applikationen online unternehmensweit verfügbar zu machen, sowie die wachsende Bedeutung von effizienten IT-gestützten Prozessen als Wettbewerbsvorteil.

Auch wenn die öffentliche Diskussion über IT-Sicherheit oft aus der Sicht der privaten Anwender geführt wird, sind **Privathaushalte** im europäischen Raum mit einem Umsatzanteil von 6% für die IT-Sicherheitsbranche nur ein Randsegment. Insgesamt ist jedoch mittlerweile die Mehrheit der privaten IT-

[5] Forrester, Market Overview IT-Security, 2009

Nutzer über potenzielle IT-Sicherheitsrisiken informiert. Die Verbreitung von einfachen IT-Sicherheitsprodukten beim Endkunden ist relativ hoch. Im europäischen Raum fokussiert sich die Nachfrage zu 81% auf einzelne Basislösungen wie Antivirus-, Antispam- und Firewallprodukte und zu 67% auf Paketlösungen, sogenannte „All-in IT-Sicherheits-Suiten".[6] Weiterführende bzw. alternative Schutzmaßnahmen für den privaten Computer werden allerdings nur von einer Minderheit als notwendig angesehen.[7] Weitere IT-Sicherheitsprodukte werden meist im Verbund mit anderen Produkten verkauft: z. B. Firewall im PC-Betriebssystem oder integrierter W-LAN Schutz im DSL Router.

Die **Privatwirtschaft** ist mit einem Umsatzanteil von rund 75%[8] der Hauptabnehmer von IT-Sicherheitsprodukten und -lösungen. Innerhalb dieses Marktsegments ist die aktuelle Nachfrage sowie die Wachstumserwartung insbesondere in der Dienstleistungsbranche hoch (z. B. Telekommunikation, Finanzdienstleistungen). Die Nachfrage von Produktions- und Konsumgüterunternehmen ist im Vergleich dazu als signifikant geringer einzuschätzen. Das erwartete durchschnittliche Wachstum liegt für die nächsten Jahre je nach Branche zwischen 9% und 14%.[9]

Neben der Privatwirtschaft ist die **öffentliche Hand** mit einem Umsatzanteil von 19% ein wichtiger Abnehmer für die IT-Sicherheitsbranche. Hier sind vor allem Produkte im Bereich Hochsicherheit relevant. Die Nachfrage in diesem Segment richtet sich in einigen Bereichen angesichts der hier berührten nationalen Sicherheitsinteressen auch besonders an inländische Unternehmen. Wegen dieses Sektors sowie aufgrund weiterer IT-Großprogramme wie E-Government-Initiativen u. Ä. wird im öffentlichen Sektor mit 16% ein höheres Nachfragewachstum als im Privatwirtschaftssegment erwartet.[10] So sind z. B. in Deutschland im Konjunkturpaket II der Bundesregierung auch dedizierte Investitionen für IT-Sicherheit vorgesehen.

---

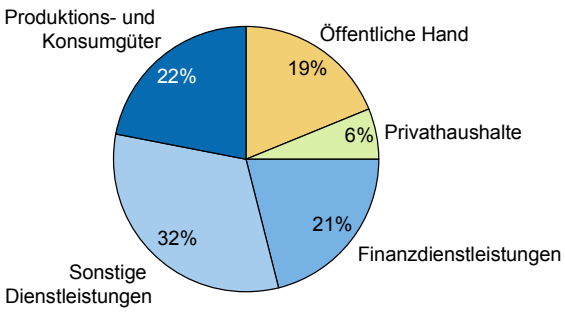
[6] IDC, The European Network and Information Security Market, 2009

[7] Gallup Organization/European Commission, Confidence in the Information Society, 2009

[8] IDC, The European Network and Information Security Market, 2009

[9] IDC, The European Network and Information Security Market, 2009

[10] IDC, The European Network and Information Security Market, 2009



Wachstumserwartung 2007-2010

Sektor	Wachstum-erwartung
Öffentliche Hand	16,3 %
Privathaushalte	10,9 %
Produktions- und Konsumgüter	13,4 %
Finanzdienstleistungen	8,8 %
Sonstige Dienstleistungen	14,1 %

Abbildung 9: Anteile der IT-Sicherheitsumsätze nach Marktsegmenten[11]

4.2 Quantifizierung des Marktes für IT-Sicherheit

4.2.1 Methodisches Vorgehen

Im Rahmen dieser Studie wurden insbesondere Primärstudien von International Data Corporation (IDC), Forrester und Experton herangezogen. Diese wurden in Gesprächen mit den Analysten sowie weiteren Experten aus Anbieterunternehmen und Forschung methodisch hinterfragt, mit deutschlandspezifischen Elementen ergänzt und die Ergebnisse plausibilisiert. Auf dieser Basis wurde eine Gesamtabschätzung im Hinblick auf die Größe, Aufteilung und Entwicklung des deutschen Marktes abgeleitet.

Hinsichtlich der Ermittlung der Gesamtumsätze im weltweiten Markt für IT-Sicherheit sind derzeit die Analystenhäuser Forrester und IDC aktiv. Dabei handelt es sich jedoch nicht um genaue statistische Erhebungen, sondern vielmehr um Abschätzungen, die auf Umfragen, Einzelgesprächen sowie auf den öffentlich zugänglichen Informationen in Jahres- und Quartalsberichten basieren.

Bei IDC liegt der Schwerpunkt auf der Anbieterseite: Für die Abschätzung werden Umsatzdaten von mehreren hundert spezialisierten Anbietern der IT-Sicherheit wie Symantec, McAfee oder CheckPoint berücksichtigt, aber auch die anteiligen Umsätze der Unternehmen, für die IT-Sicherheit nur ein Teilsegment darstellt (z. B. IBM, Microsoft oder Nokia), mit einbezogen. Da es im IT-Sicherheitsmarkt viele kleine Spezial- und Nischenanbieter gibt, wird auf der Basis dieser Erhebung nur ca. 75–80% des Marktvolumens abgeleitet. Die

[11] IDC, The European Network and Information Security Market, 2009

Angaben zum verbleibenden Teil des Marktes basieren auf reinen Schätzungen.[12]

Forrester stützt die Marktquantifizierung im Gegensatz dazu auf die Abfrage der IT-Sicherheitsbudgets von Unternehmen auf der Nachfrageseite und nimmt somit die Anwenderperspektive ein. Die Nachfrage von Privatpersonen wird nicht eingeschlossen. Zudem werden die Umsätze mit der öffentlichen Verwaltung insbesondere hinsichtlich der Dienstleistungen nur bedingt berücksichtigt, da diese oft in den allgemeinen Sicherheitsbudgets abgebildet werden. Die Ergebnisse werden anhand von Interviews mit Dienstleistungsfirmen (Anbieter von Managed Security Services und Beratungen) sowie durch Expertenbefragungen erhärtet. Da jedes Unternehmen ein potenzieller Abnehmer von IT-Sicherheitsprodukten ist, basiert die Quantifizierung zu einem großen Teil auf der Hochrechnung von Beispieldaten sowie auf Schätzungen.[13]

Für den deutschen Markt veröffentlicht lediglich das Marktforschungs- und Beratungshaus Experton eine qualifizierte Einschätzung zur Marktgröße auf der Grundlage von Unternehmensangaben über die Höhe der IT-Sicherheitsbudgets. Die Definition des IT-Sicherheitsmarktes bei Experton kommt der Abgrenzung nahe, die in dieser Studie verwendet wird. Die Unterschiede sind insbesondere die Berücksichtigung von Backup- und Recovery-Produkten (250 Mio. Euro) sowie Dienstleistungen und der Ausschluss der Nachfrage von Privathaushalten (wie erwähnt ca. 5% der Gesamtnachfrage).

Diese Studie orientiert sich im Folgenden an dem Zahlenwerk von IDC, vor allem aufgrund der dort angewandten Methodik der Datenerhebung: Die ICD-Analyse basiert nur zu einem geringeren Teil auf Exploration und Schätzungen, da die Anzahl der Unternehmen auf der Angebotsseite deutlich niedriger und damit besser eingrenzbar ist als auf der Nachfrageseite (die bei Forrester und Experton den Gegenstand der Untersuchung darstellt). Zudem bezieht diese Datenerhebung die Ebene der Untersegmente und Regionen differenziert mit ein und wagt auch eine Prognose für mehrere Jahre (bis 2012).

[12] Interview mit IDC Analysten, 2009
[13] Interview mit Forrester Analysten, 2009

4.2.2 Der weltweite Markt für IT-Sicherheit

Für die Einordnung der deutschen Anbieter von IT-Sicherheit ist auch die Betrachtung des weltweiten Markts relevant, da es sich grundsätzlich um internationale Absatzmärkte handelt. Hierzu kann das bereits oben erwähnte Zahlenmaterial von IDC und Forrester herangezogen werden.

Das Ergebnis der Markteinschätzung beider Analystenhäuser ist sehr unterschiedlich. Während IDC für das Jahr 2008 von einem weltweiten Umsatz von rund 33 Mrd. Euro ausgeht, schätzt Forrester das Marktvolumen auf lediglich 21 Mrd. Euro und liegt damit um 37% unter der Einschätzung von IDC. Im Rahmen dieser Studie werden die von IDC vorgelegten Zahlen zur Marktgröße als relevanter angesehen, insbesondere auch deshalb, weil bei IDC – wie auch in der vorliegenden Studie - die Angebotsseite des Marktes betrachtet wird (siehe auch Abschnitt 4.2.1).

Auf der Ebene der Marktsegmente besteht eine unterschiedliche Einschätzung insbesondere bei den Dienstleistungen, für die der Markt bei IDC um 42% größer eingeschätzt wird als bei Forrester (vgl. Abbildung 10).

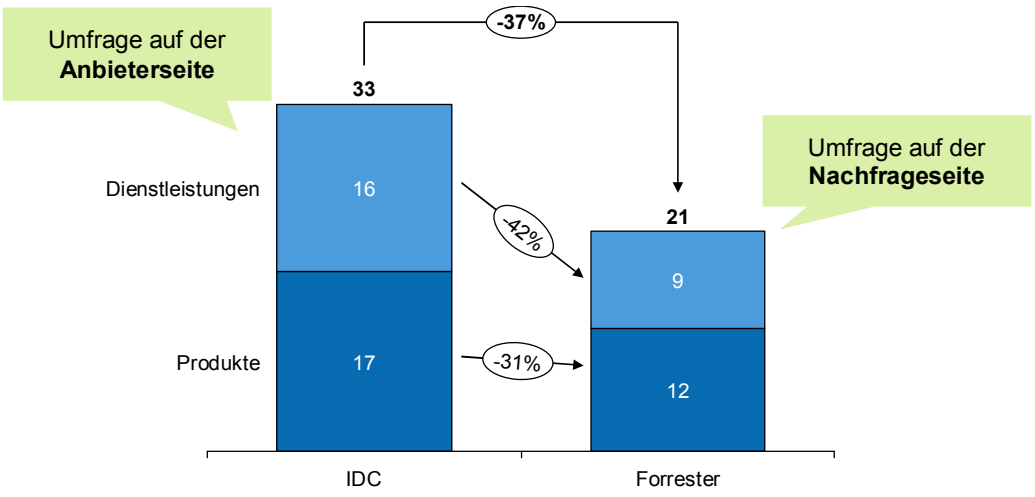


Abbildung 10: Quantifizierung des weltweiten IT-Sicherheitsmarktes durch IDC und Forrester für 2008 (in Mrd. Euro)[14]

Die Definition von IT-Sicherheit ist in beiden Erhebungen ähnlich: Beide Studien berücksichtigen sowohl IT-Sicherheitsprodukte als auch -

[14] IDC, Worldwide IT Security Software, Hardware, and Services, 2009; Forrester, Market Overview IT Security, 2009

dienstleistungen. Sie teilen den Markt in nahezu identische Segmente ein (und diese sind auch weitgehend vergleichbar mit denen, die in dieser Studie verwendet werden). Da auch die Unterschiede in der Marktabgrenzung gering sind, ist die Differenz zwischen den Studien im Wesentlichen auf die Methodik der Datenerhebung und die grundsätzlich schwierige Datenlage zurückzuführen.

Hinsichtlich der Wachstumsprognose für 2009 gehen beide Studien von einem knapp zweistelligen Wachstum aus. Ein ähnliches Wachstum wird von IDC auch für die Folgejahre bis 2012 erwartet. Forrester publiziert keine weiterführende Prognose.

Tabelle 10: Wachstumsprognosen weltweiter IT-Sicherheitsmarkt IDC und Forrester[15]

	IDC		Forrester
Segment	**Wachstum 2008–2009**	**Ø Wachstum 2008–2012 (CAGR)**	**Wachstum 2008–2009**
Produkte	9,7%	10,4%	9,8%
Dienstleistungen	17,2%	17,1%	10,6%
Gesamt	11,6%	13,4%	10,2%

Im Bereich der Dienstleistungen wird von IDC mit 17% ein deutlich stärkeres Wachstum erwartet. Grund dafür ist die Annahme, dass Firmen vermehrt auf externe IT-Dienstleistungsanbieter zurückgreifen. Durch die zunehmende Komplexität der IT-Sicherheit, so die Annahme, wird es schwieriger, selbst kompetentes Personal einzustellen und zu halten. Dies gelte insbesondere für kleine und mittelgroße Unternehmen.

Für den Untersuchungskontext dieser Studie kann für 2008 von einer weltweiten Marktgröße von 33 Mrd. Euro ausgegangen werden. Das Wachstum im Produktbereich kann im Konsens mit ca. 10% angegeben werden. Im Dienstleistungsbereich sollte von ca. 17% Wachstum ausgegangen werden.

[15] IDC, Worldwide IT Security Software, Hardware, and Services, 2009; Forrester, Market Overview IT Security, 2009

4.2.3 Der europäische Markt für IT-Sicherheit

Zum europäischen Markt für IT-Sicherheit ist nur begrenzt Zahlenmaterial vorhanden. Eine aktuelle Studie von IDC beziffert den gesamteuropäischen Markt für IT-Sicherheit auf 11 Mrd. Euro.[16] Die EU-Länder wurden dabei von IDC, basierend auf dem jeweiligen Entwicklungsstand der IT-Industrie (Pro-Kopf-Ausgaben für IT und prozentualer Anteil der IT-Ausgaben am Bruttosozialprodukt), in vier Gruppen eingeteilt. Danach sind europaweit Dänemark, Finnland, die Niederlande, Schweden und Großbritannien die am weitesten entwickelten IT-Märkte mit den höchsten relativen Ausgaben für IT-Sicherheit. Deutschland sowie Frankreich, Österreich, Belgien und Irland werden aufgrund etwas geringerer Pro-Kopf-Ausgaben für die IT-Sicherheit der zweiten Gruppe zugeordnet. Ein deutlicherer Unterschied hinsichtlich des IT-Entwicklungsstandes besteht im Vergleich zu den Ländern der dritten Gruppe, zu der u. a. Italien, Spanien und Griechenland gezählt werden. In diesen Ländern ist auch der Serviceanteil der IT-Ausgaben geringer, was als ein Indikator für den niedrigeren Reifegrad der Märkte angesehen werden kann. In den osteuropäischen Ländern, die wiederum in der vierten Gruppe zusammengefasst werden, ist der IT-Sicherheitsmarkt noch unterentwickelt. Lediglich 2% der Umsätze des gesamten EU-Marktes wird in diesen Ländern erzielt (Einwohneranteil 16%). Hier wird jedoch andererseits auch mit einem jährlichen Umsatzwachstum von durchschnittlich 20% die stärkste Steigerung erwartet.

Bricht man die Ergebnisse der Studie auf Länderebene herunter (unter der Annahme, dass sich die IT-Sicherheitsausgaben der einzelnen Länder innerhalb der Gruppen proportional zu den Anteilen des jeweiligen Bruttoinlandsprodukts verhalten) ergibt sich folgendes Bild: Auf Länderebene ist Großbritannien mit 2,8 Mrd. Euro (2008) der größte Markt für IT-Sicherheit in Europa, gefolgt von Deutschland (2,5 Mrd. Euro) und Frankreich (2,2 Mrd. Euro). Der Grund für die relative Stärke Großbritanniens – dessen Volkswirtschaft ja kleiner als die deutsche ist – liegt im grundsätzlich höheren Anteil an IT und Dienstleistungen an der Gesamtwirtschaft (vgl.
Abbildung 11).

[16] IDC, The European Network and Information Security Market, 2009

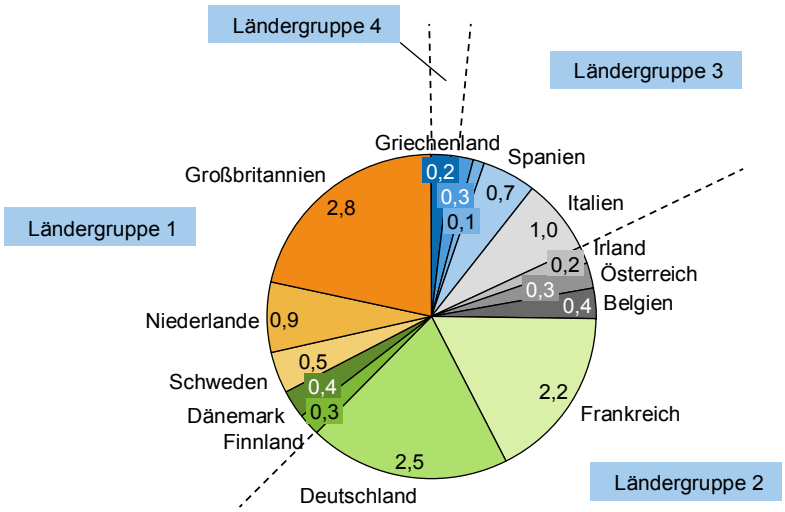


Abbildung 11: Europäischer Markt für IT-Sicherheit 2008 (in Mrd. Euro), gruppiert nach Ländergruppen mit ähnlichen Pro-Kopf-IT-Ausgaben [17]

Die Annahmen von IDC für die Marktquantifizierung auf europäischer Ebene erscheinen valide und können zur Plausibilisierung der Untersuchung für den deutschen Markt herangezogen werden (vgl. den folgenden Abschnitt).

4.2.4 Ansatz zur Quantifizierung des deutschen Marktes für IT-Sicherheit

Detaillierte Zahlen für den deutschen Markt, die die Anbieterseite betrachten, liegen nicht vor. Auf der Basis der internationalen und europäischen Studien von IDC und Forrester sowie der nachfrageorientierten Schätzungen von Experton für Deutschland kann jedoch trotzdem eine Einschätzung getroffen werden.

Um aus den internationalen Zahlenwerken eine Marktabschätzung für Deutschland abzuleiten, wurde der Anteil des deutschen IT-Marktes am globalen IT-Markt (ca. 7%) zugrunde gelegt. Bedingt durch methodische Unterschiede ergibt sich damit für den deutschen Markt noch eine Einschätzungsbandbreite in 2008 von 1,6 (Forrester) bis 3,6 (Experton) Mrd. Euro. Die Einschätzung von IDC liegt mit 2,3 Mrd. Euro nahezu in der Mitte.

[17] IDC, The European Network and Information Security Market, 2009

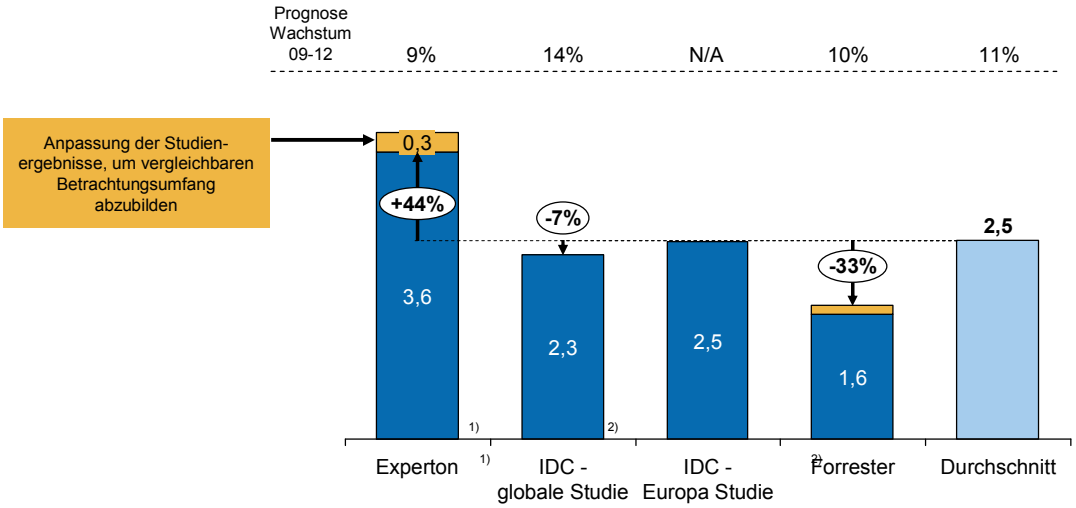


Abbildung 12: Deutscher Markt für IT-Sicherheit 2008 und Wachstumsprognose bis 2012 (in Mrd. Euro)[18]

Analog zu den Einschätzungen zum Weltmarkt ist der Unterschied zwischen den Studien für die Dienstleistungen besonders hoch. Dies ist vor allem auf die größere Intransparenz hinsichtlich der Nachfrage in diesem Segment zurückzuführen.

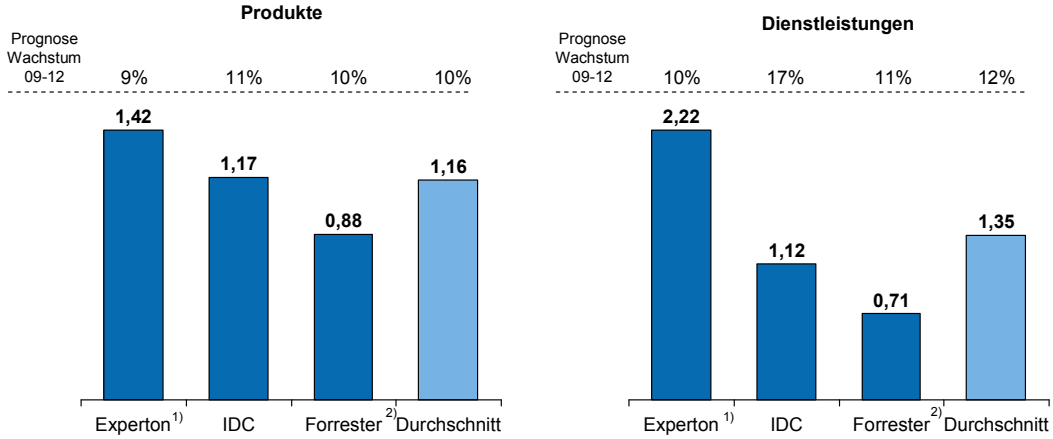


Abbildung 13: Deutscher Markt für IT-Sicherheit 2008 (Produkte und Dienstleistungen) und Wachstumsprognose bis 2012 (in Mrd. Euro)[19]

---

[18] IDC, Worldwide IT Security Software, Hardware, and Services, 2009; Forrester, Market Overview: IT Security, 2009 (um Dienstleistungen für Regierungsorganisationen und Nachfrage Privathaushalte angepasst); Experton, Informationssicherheit trotz(t) der Krise, 2009 (um Backup und Recovery Umsätze und Nachfrage Privathaushalte angepasst)

[19] IDC, Worldwide IT Security Software, Hardware, and Services, 2009; Forrester, Market Overview: IT Security, 2009 (bezüglich der Dienstleistungen für Regierungsorganisationen und die Nachfrage der Privathaushalte angepasst); Experton, Informationssicherheit trotz(t) der

Die langfristige Gesamtwachstumsprognose liegt zwischen 9% (bei Experton) und 14% (bei IDC). Dieser Unterschied ist auf die höhere Wachstumsprognose von IDC in Bezug auf die Dienstleistungen zurückzuführen, die mit 17% deutlich über den Annahmen von Experton und Forrester liegt (zu den Gründen vgl. Abschnitt 4.2.1). Die Wachstumsprognose für IT-Sicherheitsprodukte liegt bei allen Studien nahezu identisch bei jährlich 9–11%. Lediglich im Jahr 2009 wird, bedingt durch die Wirtschaftskrise, im Allgemeinen ein etwas reduziertes Wachstum erwartet. So geht Experton beispielsweise von einem 6%igen Wachstum im Jahr 2009 aus.

Zusammenfassende Einschätzung:

Zusammenfassend lässt sich damit jedenfalls feststellen, dass der deutsche Markt für IT-Sicherheit mit einem in absehbarer Zeit konstanten jährlichen Wachstum von ca. 10% ein attraktives Geschäftsfeld darstellt. Die Größe des Marktes kann aufgrund der intransparenten Datenlage und der im Abschnitt 4.2.1 beschriebenen Probleme bei der Quantifizierung sowohl auf der Nachfrage- als auch auf der Angebotsseite allenfalls innerhalb einer gewissen Bandbreite von Möglichkeiten eingeschätzt werden.

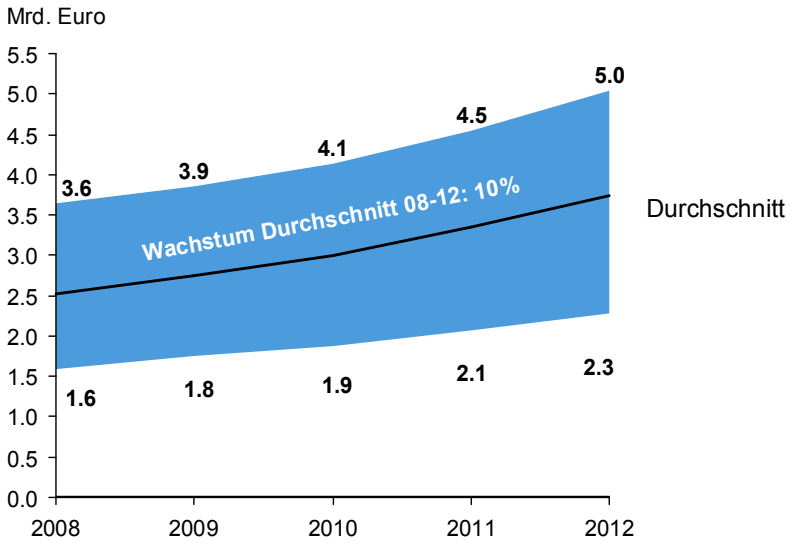


Abbildung 14: Bandbreite der Gesamtumsätze des deutschen IT-Sicherheitsmarktes

Im Untersuchungskontext dieser Studie soll hierbei von einer Marktgröße von ca. 2,5 Mrd. Euro im Jahre 2008 ausgegangen werden. [20]

Krise, 2009 (bezüglich der Backup- und Recovery-Umsätze und der Nachfrage der Privathaushalte angepasst)

[20] Quelle: Darstellung Booz & Company

4.3 Die aktuelle Entwicklung der Bedrohungslage

Für die Einschätzung des IT-Sicherheitsmarktes sowie die Chancen deutscher Anbieter ist eine eingehende Analyse der aktuellen und künftigen Bedrohungslage erforderlich, da der Bedarf an IT-Sicherheitsprodukten und -dienstleistungen zu einem erheblichen Teil durch diese determiniert wird. Im Rahmen der Studie wurde die Entwicklung der Gefährdungslage im Hinblick auf Gefährdungstrends, Schutzbedarfe neuer Technologien und kritische Infrastrukturen beleuchtet. Eine detaillierte Untersuchung zu den einzelnen Bereichen findet sich in Anhang der Studie (Abschnitt 9.18). Im Rahmen der Untersuchung haben sich jedoch drei besonders relevante übergreifende Trends herauskristallisiert.

Zunehmende Professionalisierung bzw. Industrialisierung der Angriffe

Es gibt mittlerweile eine Reihe von Anzeichen, die auf eine zunehmende Professionalisierung der Angriffe hindeuten. Dies betrifft zum einen die Herangehensweise der Angreifer:

- Angriffe werden vermehrt **gezielt geplant und zentral gesteuert** (z. B. mittels verteilter Bot-Netze, die durchaus mehr als 1 Mio. infizierte Rechner umspannen können).
- Neu entdeckte **Sicherheitslücken werden sehr schnell ausgenutzt** (sog. „Zero Day Exploits").
- Die Angreifer verwenden zunehmend **nachrichtendienstliche Methoden** (z. B. „Social Engineering"), um Angriffsziele vorher auszukundschaften.
- Angriffe erfolgen verstärkt aus **kommerziellen Interessen**. Mittlerweile werden derartige Angriffe und die Nutzung der entsprechenden Werkzeuge als Dienstleistung gegen Entgelt angeboten. Hierbei erfolgt die Preisbildung nach Art eines funktionierenden Marktes durch Angebot und Nachfrage.[21]

Eine Professionalisierung ist jedoch nicht nur im Vorgehen zu beobachten, sondern auch bei den eingesetzten Schadprogrammen und Werkzeugen:

[21] G Data, Underground Economy G Data, Whitepaper 2009, Underground Economy

- Die Schadprogramme weisen immer **kürzere Entwicklungszyklen** auf, sind **modular aufgebaut** und aktualisieren sich selbst über **integrierte Update-Funktionen**.
- Im Extremfall können speziell konfigurierte Schadprogramme **„on demand" im Internet erzeugt werden** – selbst von nicht fachkundigen Personen.
- Die Entwickler von Schadprogrammen versuchen gezielt, der Erkennung zu entgehen, und implementieren entsprechende **Tarnfunktionen** (z. B. als Rootkits, polymorphe serverseitige Viren).

Steigende Durchdringung des beruflichen und privaten Alltags durch die IT

Die Informationstechnologie durchdringt im steigenden Maße den beruflichen und auch den privaten Alltag („ubiquitous computing"). Dadurch betreffen auch IT-Sicherheitsproblematiken immer größere Teile des Alltags. Dieser Trend wird von einer Vielzahl von Faktoren gestützt:

- IT-Anwendungen werden verstärkt auch auf **mobilen Endgeräten** (z. B. PDAs, Smartphones) eingesetzt.
- Mit der zunehmenden **Verfügbarkeit breitbandiger Internetanbindungen** und darauf aufbauenden Angeboten (z. B. IP-TV) steigt die Internetnutzung allgemein.
- Damit einher geht die Auflösung der Grenze zwischen Informationsanbietern und -nutzern durch **Web-2.0-Applikationen** wie WIKIs und soziale Netzwerke.
- Durch die **Konvergenz von Telekommunikations- und Informationstechnologie** (z. B. Voice over IP) treten neue IT-Sicherheitsherausforderungen auf (z. B. Spam over VoIP).
- Der gegenwärtige Trend, die Bereitstellung von IT-Anwendungen zu virtualisieren und den Speicherort von Daten zu flexibilisieren (z. B. in Form von **Cloud Computing**), führt zu einer Aufweichung der Außengrenzen (engl. perimeter) von Unternehmensnetzen und Anwendungen. Solche Anwendungen können nur schwer mit einem undurchdringlichen Schutzwall aus Firewalls, Intrusion Detection Systems (IDS), Content Filtering, Application Hardening und Data-Loss-Prevention-Systemen versehen werden.

- Zuletzt dehnt sich die IT- und Internettechnologie zunehmend auf den Bereich **Steuerungselektronik** (z. B. in modernen Fahrzeugen und Versorgungsinfrastrukturen, sog. „Smart Grids") und im Sinne des **„Internets der Dinge"** auf nahezu alle elektronischen Gerätschaften aus.

Steigende Bedeutung von Identitätsmanagement

Die Identifikation von Personen bzw. die Sicherstellung ihrer Identität ist ein Bereich, der im Internet, aber auch in der Informationstechnologie allgemein einen zunehmenden Stellenwert erlangt. Die Zahl der Fälle von Identitätsdiebstahl hat deutlich zugenommen. Für Identitäten im Rahmen von Online-Rollenspielen und für Kreditkartenidentitäten existiert bereits ein funktionierender Markt.[22]

Die steigende Bedeutung des Identitätsmanagements ergibt sich auch aus der zunehmenden Verbreitung biometrischer Verfahren und der eID-Funktionen des elektronischen Personalausweises. Diese Verfahren stellen aus der Sicht des Datenschutzes neue Herausforderungen dar, bieten jedoch auch für die Anbieter neue Chancen.

[22] G Data, Underground Economy G Data, Whitepaper 2009, Underground Economy

4.3.1 Aktuelle Schwachstellen und Bedrohungen von IT-Systemen

Die folgende Tabelle gibt einen Überblick über die derzeitigen akuten Gefährdungstrends, geordnet nach der Art der Bedrohung (Spezifizierung in Abschnitt 8.1, im Anhang):

Tabelle 11: Gefährdungstrends in der IT-Sicherheit[23]

Bedrohung	2007	2009	Progn.
Zero Day Exploits	↑	↑	→
Drive-by-Downloads	-	↑	↑
Trojanische Pferde	↑	↑	↑
Viren	↓	↓	→
Würmer	↓	↓	→
Spyware	↑	↑	→
DDoS Angriffe	→	↑	↑
Unerwünschte E-Mails (Spam)	↑	↑	↑
Botnetze	→	↑	↑
Identitätsdiebstahl	↑	↑	↑
Betrügerische Webangebote	-	↑	→

↑ Steigend
→ Gleichbleibend
↓ Abnehmend

Der Umgang mit der IT Sicherheit innerhalb vieler Unternehmen kann als problematisch bezeichnet werden. In einer vom BMWi geförderten und im Oktober 2008 veröffentlichten Umfrage des E-Commerce Center Handel (ECC) und des Netzwerk Elektronischer Geschäftsverkehr (NEG) zur Informationssicherheit in Unternehmen in 2008, gaben über die Hälfte der etwa 250 befragten kleinen und mittelständischen Unternehmen an, über keinen IT Sicherheitsbeauftragten zu verfügen. Etwa ein Drittel der Unternehmen hätte die Pflege des Netzwerks, der Hardware und der Firewall an externe Dienstleister ausgelagert und zudem auch keine IT Sicherheitsrichtlinie zum sicheren Umgang mit dem Computer. Zwei Drittel der Unternehmen hätten den Zugriff auf die im Unternehmen eingesetzten Computer nicht beschränkt, d.h. die USB Schnittstellen oder die CD/DVD Laufwerke gesperrt. Bedenklich war zudem, dass in drei Viertel der befragten Unternehmen betriebsfremde Personen keinen Besucherausweis tragen müssten und in jedem vierten sich diese Personen ohne Aufsicht in den Firmenräumen aufhalten könnten. Als

[23] BSI, Die Lage der IT Sicherheit in Deutschland, 2009

einen der wesentlichen Gründe für diese Nachlässigkeit gaben viele Unternehmen an, sich mit dem Thema IT Sicherheit noch nicht auseinander gesetzt zu haben.[24]

Nach Angaben des BSI kommen zudem fehlende personelle und finanzielle Ressourcen sowie technisches Know-how hinzu. Zwar seien technische Schutzmaßnahmen zur Datensicherung besonders wichtig, da Angriffe durch neue und komplexe Techniken zunehmend schwerer zu bekämpfen seien, doch auch die innovativsten technischen Sicherheitsmaßnahmen böten nur einen begrenzten Schutz, wenn Mitarbeiter oder externe Dienstleister auf Daten zugriffen und diese missbrauchten (vgl. Abbildung 15 und Abbildung 16).

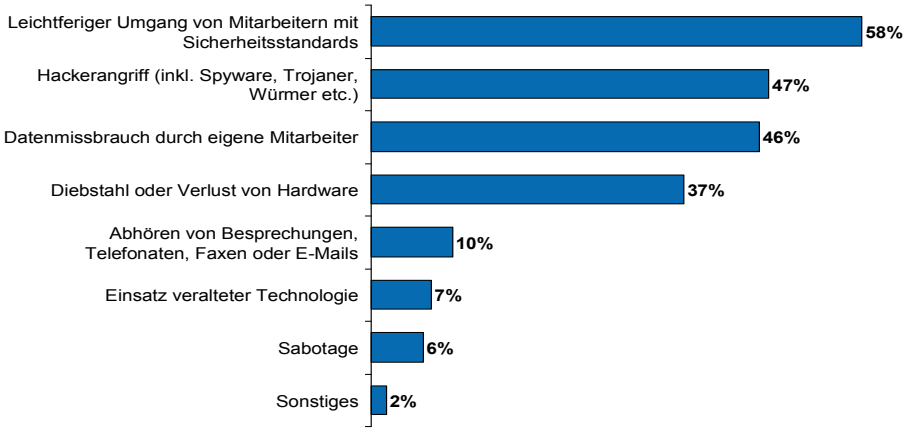


Abbildung 15: Häufigste Gefahrenquellen für die IT-Sicherheit (Mehrfachnennungen möglich)[25]

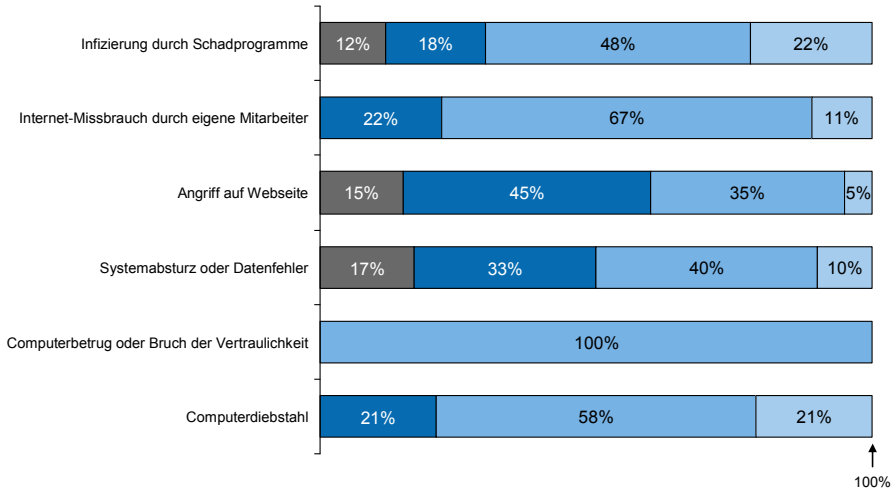


Abbildung 16: Auswirkung der Sicherheitsvorfälle auf das Unternehmen[26]

[24] E-Commerce Center Handel, „Informationssicherheit in Unternehmen, 2008“, Oktober 2008

[25] Corporate Trust Studie, 2009

Jeder einzelne Bürger und jede Einrichtung, gleich ob privat oder öffentlich, steht vor der Aufgabe, das eigene Bedrohungsrisiko einzuschätzen und die geeigneten Maßnahmen zu ergreifen. Die Abhängigkeit von der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der jeweiligen Technik ist nicht überall gleich, und die Folgen fehlender oder unzureichender IT-Sicherheitsmaßnahmen treffen jeden anders. Faktoren wie die eigene Technikaffinität und -akzeptanz sowie die eigenen Sicherheitsbedürfnisse und -kenntnisse beeinflussen das Bewusstsein und die Kompetenz der verschiedenen gesellschaftlichen Gruppen.[27]

Die nicht abnehmende Komplexität der Schnittstelle zwischen Computer und Benutzer wird ebenfalls als Bedrohung gesehen, da viele Bürger und kleine Unternehmen weder ein Interesse daran noch die nötigen Kenntnisse haben, um die Installation und Konfiguration von IT-Sicherheitssystemen und -programmen selbst vorzunehmen. Für größere Unternehmen und Behörden mit professionellem IT-Security-Management gilt dies in dieser Form nicht.

4.3.2 Neue Bedrohungsszenarien in ausgewählten Technologien

Neben den neuen oder neuerdings verstärkt vorkommenden Angriffsmöglichkeiten sind insbesondere auch neue Bedrohungsszenarien zu untersuchen, welche sich durch derzeit aufstrebende Anwendungen und Technologien ergeben. Abbildung 17 gibt einen Überblick über die erwartete Entwicklung. Die einzelnen Technologien und Anwendungen und deren Risikopotenzial werden im Anhang (Abschnitt 8) näher beschrieben.

Technologie	2007	2009	Progn.
Voice over IP	↑	→	→
Mobile Kommunikation	-	↑	↑
Web 2.0	-	↑	↑
SOA	-	↑	↑
RFID	→	→	↑
Biometrie	-	↑	↑
IPv6	-	↑	→

Abbildung 17: Risikopotential ausgewählter Anwendungen und Technologien[28]

[26] PriceWaterhouseCoopers, Information Security Breaches Survey, 2006
[27] BSI, Die Lage der IT Sicherheit in Deutschland, 2009
[28] BSI, Die Lage der IT Sicherheit in Deutschland, 2009

4.3.3 Besondere Anforderungen im Bereich „kritische Infrastruktur“

Die Informations- und Kommunikationstechnologie ist zur kritischen Infrastruktur zuzurechnen, da sie angesichts der zunehmenden Vernetzung vieler lebenswichtiger Systeme und Funktionen gleichsam das zentrale Nervensystem eines Landes darstellt.

Für die Betreiber kritischer Infrastrukturen ist es daher wichtig, die relevanten Risiken zu kennen, um eventuelle Angriffe insbesondere im IT Bereich rechtzeitig erkennen und sich darauf einstellen zu können. Das bedeutet, die gegebenen Risiken bereits im Vorfeld von konkreten Gefährdungsereignissen so weit wie möglich zu erfassen und zu mindern und sich auf unvermeidbare Krisenfälle bestmöglich vorzubereiten.

Als Reaktion auf die wachsende IT-Bedrohungslage hat die Bundesregierung 2005 den „Nationalen Plan zum Schutz der Informationsinfrastrukturen“ (NPSI) beschlossen. Der NPSI ist sozusagen die Dachstrategie zu IT-Sicherheit und sieht drei Tätigkeitsfelder vor:

- Prävention: Informationsinfrastrukturen in Deutschland angemessen schützen
- Reaktion: bei IT-Sicherheitsvorfällen wirkungsvoll handeln
- Nachhaltigkeit: die deutsche IT-Sicherheitskompetenz stärken – international Standards setzen.

Zur Realisierung der im NPSI formulierten Ziele hat das Bundesinnenministerium gemeinsam mit etwa 30 großen deutschen Infrastruktur-Unternehmen und einigen Interessenverbänden in vier Arbeitsgruppen den „Umsetzungsplan KRITIS“ erarbeitet. Ergebnisse dieser Arbeit wurden Anfang 2009 in Gestalt von Rahmenkonzepten zu „Notfall- und Krisenübungen“ sowie zu „Krisenreaktion und -bewältigung“ veröffentlicht. Die beteiligten Organisationen verpflichten sich auf freiwilliger Basis, in der IT-Sicherheit ein Mindestniveau einzuhalten.

Eine wesentliche Vorgabe des NPSI ist die Festlegung genauer Richtlinien für den Schutz der Informationsinfrastrukturen in der Bundesverwaltung durch die Bundesregierung. Mit dem „Umsetzungsplan für die Gewährleistung der IT-Sicherheit in der Bundesverwaltung“ (UP Bund) hat die Bundesregierung verbindliche IT-Sicherheitsleitlinien für die Bundesverwaltung verabschiedet.

Die zunehmende Allgegenwärtigkeit und Vernetzung der Informationstechnik im Geschäftsleben, im Behördenalltag sowie im täglichen Leben der Bundesbürger (siehe auch Abschnitt 4.3.1) erfordert umfangreiche technische und organisatorische Sicherungsmaßnahmen, um die Sicherheit von Informationen und Systemen zu gewährleisten. Mit gestohlenen personenbezogenen Informationen, Zugangsdaten oder geistigem Eigentum erzielen organisierte Kriminelle Gewinne in Milliardenhöhe[29]. Der Parlamentarische Staatssekretär im BMWi, Peter Hintze, fasst diese Situation wie folgt zusammen: „Mit den Chancen stiegen auch die Risiken. Und mit diesen Risiken müssen wir intelligent umgehen."[30]

[29] BSI, Die Lage der IT Sicherheit in Deutschland, 2009
[30] Hintze, Peter: „Sicherheit 2009 Industrialisierung der Computerkriminalität", 20.01 2009.

4.4 Aktuelle Trends auf der Nachfrageseite

Bei der Betrachtung der Trends auf der Nachfrageseite stehen zunächst die Trends hinsichtlich einer vermehrten Nachfrage in spezifischen Untersegmenten im Vordergrund (Abschnitt 4.4.1). Darauf folgend wird kurz auf den Trend der Hypervernetzung eingegangen (Abschnitt 4.4.2), bevor auf die Zunehmende Bedeutung von Datenschutz-Compliance eingegangen wird (Abschnitt 4.4.3). Abschließend folgen die technologischen Trends (Abschnitt 4.4.4) sowie eine kurze Darstellung der Auswirkungen der aktuellen Wirtschaftskrise auf die IT Sicherheitsbranche (Abschnitt 4.4.5).

4.4.1 Nachfragetrends hinsichtlich spezifischer Produkte und Dienstleistungen

Der Anteil der IT-Sicherheit am IT-Gesamtbuget der Unternehmen hat sich (nach Analysen von Forrester) in der Vergangenheit kontinuierlich vergrößert und liegt aktuell bei ca. 10%. 20% dieses Budgets wiederum werden für neue Initiativen und jeweils 24% für Upgrades bestehender Systeme sowie für Beratungs- und andere Dienstleistungen verwendet. Die verbleibenden Ausgaben entfallen auf Kosten für internes Personal (31%) und Sonstiges (1%).[31]

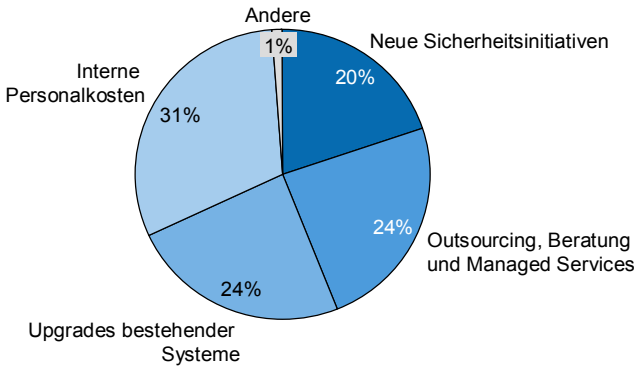


Abbildung 18: Aufteilung der IT-Sicherheitsbudgets[32]

Fokus auf die Datensicherheit

Während bislang der Fokus im Bereich der IT-Sicherheit bei vielen Unternehmen auf dem Schutz vor externen Bedrohungen (durch Firewalls, Antivi-

[31] Forrester, The State of Enterprise IT Security, 2008
[32] Forrester, Enterprise IT-Security in Europe, 2009

rus, Antispam, Antispyware etc.) lag, steht derzeit zunehmend der Schutz der Daten selbst im Vordergrund.[33] Wenn man beispielsweise den Mitarbeitern den Zugriff auf Daten auch außerhalb des Unternehmens und mobil ermöglicht oder wenn man Software-als-Service-Produkte (SaaS) nutzt, wird es komplizierter, die Außengrenze der IT-Infrastruktur zu definieren und zu schützen. Da Firmendaten oft zu den sensibelsten Werten eines Unternehmens gehören, umfassen die Schutzmaßnahmen nicht mehr allein die Verschlüsselung, sondern zunehmend auch eine verstärkte Zugriffs- und Nutzungskontrolle. Vor diesem Hintergrund werden integrierte IT-Sicherheitslösungen nachgefragt, die den Datenschutz im erweiterten Kontext des Datenmanagements beinhalten. Dabei steht sowohl der Schutz von wettbewerbsrelevanten Daten (wie z. B. Kundendatenbanken) als auch die Einhaltung von vertraglichen und gesetzlichen Verpflichtungen im Fokus. Eine aktuelle Forrester-Umfrage bestätigt, dass die IT-Verantwortlichen der Unternehmen die Datensicherheit unter den IT-Sicherheitsthemen als besonders wichtig eingestufen (vgl. Abbildung 19).[34] Insbesondere der Schutz von Kunden- sowie von wettbewerbsrelevanten Unternehmensdaten und geistigem Eigentum hat dabei eine hohe Priorität (vgl. Abbildung 20). Auf die Datensicherheit folgen in der Einstufung der Wichtigkeit die Applikationssicherheit sowie Business Continuity/Disaster Recovery.

[33] IDC, The Changing Landscape of IT Security: Emerging Trends and the Role of Israeli Innovation, 2009
[34] Forrester, Enterprise IT Security in Europe, 2009

Abbildung 19: Prioritäten im IT-Sicherheitsbereich (Einschätzung als „wichtig" oder „sehr wichtig" durch 285 IT-Sicherheitsverantwortliche in europäischen Firmen)[35]

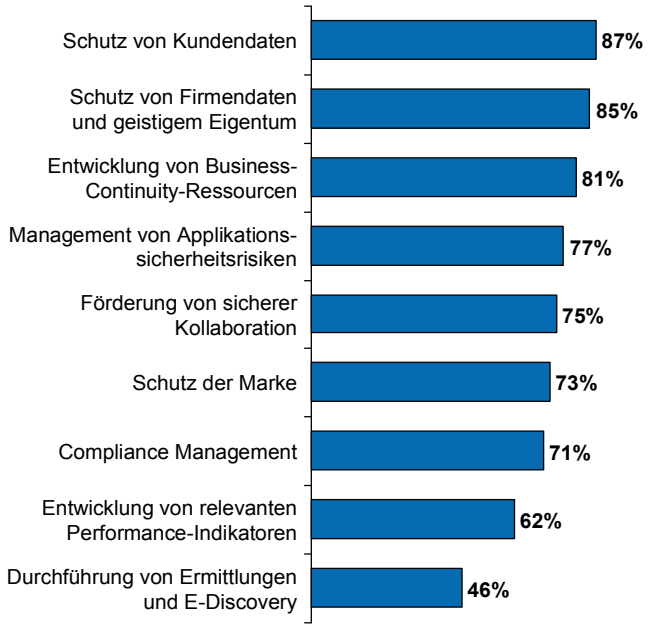


Abbildung 20: Zielprioritäten der IT-Sicherheitsorganisation[36]

[35] Forrester, Enterprise IT-Security in Europe, 2009
[36] Forrester, Enterprise IT Security in Europe, 2009

Aktuelle Vorfälle, wie die Entwendung von 130 Millionen Kreditkartennummern aufgrund von Sicherheitslücken in Datenbanken von Supermärkten und Zahlungsabwicklungsfirmen, bestätigen die Dringlichkeit eines effektiveren Schutzes von Unternehmensdaten.[37] Schwierigkeiten sehen Führungskräfte oft bei der Implementierung der richtigen Prozesse, der Suche nach geeignetem Personal sowie bei der internen Rechtfertigung der Kosten.

Managed Security Services

Das Interesse an Managed Security Services wächst vor dem Hintergrund des zunehmenden Stellenwerts und der wachsenden Komplexität der IT-Sicherheit besonders stark. Abgesehen von den traditionell fremdvergebenen Funktionen wie Firewall Control oder Content Security ist vor allem die Nachfrage nach integrierten Lösungen für Netzwerksicherheit gestiegen. Hier wird auch in Zukunft das stärkste Wachstum erwartet. Darüber hinaus suchen Unternehmen vermehrt nach externen Lösungen für Vulnerability Management, Endpoint Security oder Identity Management auch als Software-as-a-Service-Angebot.[38]

In die Sicherheitspolitik der Unternehmen werden dagegen seltener externe Dienstleister involviert. Aber auch für andere Bereiche wird die Auslagerung von Sicherheitsleistungen von vielen IT-Leitern immer noch kritisch betrachtet. So werden bei zwei Dritteln aller Unternehmen sämtliche Aufgaben im Zusammenhang mit der IT-Sicherheit von eigenen Mitarbeitern durchgeführt. Unternehmen, die bereits auf Drittanbieter für IT-Sicherheit zurückgreifen, haben ihre Outsourcing-Aktivitäten allerdings meist intensiviert.[39] Hier zeigt sich, dass die Fremdvergabe von Spezialaufgaben wie IT-Sicherheit oftmals wirtschaftlich sinnvoll ist. Funktionen, die bevorzugt ausgelagert werden, sind das Management von Firewall, Messaging und VPN. Dabei liegt der Fokus auf der Fernüberwachung sowie der Verwaltung von Systemen, die im Rechenzentrum des Anwenders betrieben werden.[40] Allerdings birgt der Zugriff externer Firmen auf Unternehmensdaten im Rahmen des Outsourcings auch zusätzliches Gefahrenpotenzial. Umfragen zufolge haben viele Unternehmen weder den genauen Überblick über externe Zugriffsrechte, noch haben sie überprüft, ob der Outsourcing-Dienstleister die relevanten Daten-

[37] Financial Times Deutschland, Größter Kreditkartenklau in den USA, 19.08.09
[38] Forrester, Market Overview: IT Security, 2009
[39] Capgemini, IT-Trends, 2009
[40] Computerwoche, Sicherheit in Krisenzeiten, 2009

schutzanforderungen erfüllt.[41] Bei Cloud Computing können vor allem kleine und mittlere Unternehmen (KMU) von der Spezialisierung und der Erfahrung der Anbieter in der Implementierung und im Betrieb von sicheren Services und von der Möglichkeit der Ausnutzung von Skaleneffekten profitieren. Allerdings stehen diese Cloud Services in der Regel nur über standardisierte Service Level Agreements (SLA) ohne ausgeprägte Sicherheitsgarantien zur Verfügung, die im Falle von KMUs nicht frei verhandelt werden sondern nur akzeptiert oder ablehnt werden können.[42]

Zunehmende Durchführung von Awareness-Trainings

Sicherheitsrelevantes Fehlverhalten von eigenem Personal gilt mittlerweile als eine der größten Schwachstellen der IT-Sicherheit. Um das Sicherheitsbewusstsein zu erhöhen, setzen daher mittlerweile 40–60% der Unternehmen auf Awareness-Maßnahmen und Schulungen, und zwar mit steigender Tendenz.[43] Welches Sicherheitsrisiko vom internen Personal ausgeht, zeigt u. a. das Beispiel des Computerwurms Conficker, der über einen USB-Stick eines Mitarbeiters auf einen Server der Bundeswehr gelangte und dort erhebliche Probleme verursachte.[44]

Steigerung der Effizienz im IT-Sicherheitsbereich

Im Zusammenhang mit einer zunehmenden Beachtung der IT-Sicherheit durch das Top-Management gibt es vermehrt Bestrebungen, diese wirksamer an die individuellen Anforderungen des Unternehmens anzupassen.[45] Dazu wird der IT-Sicherheitsbereich u. a. verstärkt in den gesamten IT-Betrieb und in die Organisation der physischen Sicherheit integriert. Im Rahmen dieser Entwicklung wird z. B. eine Integration der Sicherheit von Sprach-, Video und Datenkommunikation durchgeführt oder eine Verbindung zwischen den Personaldaten in Human-Resources-Datenbanken mit Identity-Access-Management-Programmen in physischen Zugangkontrollsystemen hergestellt. Gleichzeitig werden physische Sicherheitskontrollsysteme genutzt, um Schadens- und Betrugsfälle im Bereich der IT besser analysieren zu können. Um die Effizienz der IT-Sicherheit enger zu kontrollieren, hat die Mehrheit

---

[41] PWC, The Global State of Information Security, 2008
[42] Fraunhofer Institut für IT Sicherheit, Cloud Computing Sicherheit, 2009

[43] Deloitte, TMT Global Security Survey, 2009; Capgemini, IT-Trends, 2009; PWC, The Global State of Information Security, 2008
[44] eGovernment, Mensch und Maschine arbeiten noch nicht Hand in Hand, 2009
[45] Forrester, Enterprise IT Security, 2008

der Unternehmen bereits Kennzahlen über die Sicherheitsanfälligkeit in das IT-Reporting integriert.[46]

4.4.2 Trend zur Hypervernetzung

Der Terminus „Hypervernetzung" bezeichnet die durchgängige Erreichbarkeit von Personen sowie die Nutzung von mehreren mobilen Geräten (wie Laptop, PDA oder Handy) und Anwendungen (E-Mail, Instant Messaging, VoIP, Social Networking). Nach einer Studie des Herstellers Nortel sind derzeit ca. 16% aller Arbeitnehmer „hypervernetzt". Es wird erwartet, dass dieser Anteil, insbesondere durch die Weiterentwicklung der Vernetzung im privaten Umfeld, bald auf 50% steigt.[47] Durch diese Entwicklung entstehen neue Angriffspotenziale, die neuartige Sicherheitslösungen für mobile und stationäre Endgeräte erfordern.

4.4.3 Zunehmende Bedeutung von Datenschutz-Compliance

Die Relevanz des Schutzes von personenbezogenen Daten hat im Rahmen der Digitalisierung und der weltweiten Vernetzung zugenommen. Oft ist den handelnden Personen nicht bewusst, dass bei fast allen elektronischen Transaktionen automatisch personenbezogene Daten generiert und gespeichert werden. Lidl, Deutsche Bahn, Deutsche Telekom, Deutsche Bank – die zahlreichen und vielbeachteten Datenschutzskandale des letzten Jahres zeigen, dass ein wirksamer Datenschutz umfangreiche interne Strukturen erfordert, die die Einhaltung der gesetzlichen Rahmenbedingungen gewährleisten. Gleichzeitig stellt die zunehmende Verlagerung von IT-Aufgaben in Länder ohne ausreichende Datenschutzgesetzgebung die Einhaltung und Überprüfung dieser Vorgaben in Frage.

Jedenfalls gehört zu den aktuellen Herausforderungen im Bereich der IT-Sicherheit neben den Bedrohungen von außen auch die Vielzahl der gesetzlichen Vorgaben zum Datenschutz. So gilt seit dem 1. September 2009 ein verändertes Bundesdatenschutzgesetz, welches die Anforderungen an die Unternehmen zum Schutz der personengebozenen Daten weiter erhöht. Die neue Norm enthält nunmehr eine Informationspflicht gegenüber den Auf-

[46] Capgemini, IT-Trends, 2009

[47] Nortel, Hyperconnectivity leads to enterprise transformation, 2009 (obwohl nicht explizit angegeben, dürfte sich diese Zahl nur auf die weiter entwickelten Industrienationen beziehen)

sichtsbehörden und den Betroffenen, Datenschutzverletzungen zu melden und zu veröffentlichen.

Insgesamt erwartet das Marktforschungsunternehmen Gartner in den kommenden zwei Jahren stärkere staatliche Vorgaben im Bereich der IT-Sicherheit. Anbieter und IT-Abteilungen sind darauf jedoch – nach der Einschätzung von Gartner – bislang nicht ausreichend vorbereitet.[48] Diese Vorhersage wird gestützt durch Vorhaben der neuen Bundesregierung, über die bereits beschlossenen Änderungen hinaus den Schutz personenbezogener Daten weiter zu verstärken. Zudem sind Änderungen bei der Haftung von System- und Dienstanbietern für die IT Sicherheit geplant, zum Vorteil der Endanwender.[49]

4.4.4 Technologische Trends

Software as a Service / Cloud Computing

Auch wenn viele Unternehmen Cloud Computing[50] noch mit Skepsis gegenüberstehen, kommt dieses Konzept in unterschiedlichen Formen zunehmend zum Einsatz. Auf der Angebotsseite entstehen neben den Software-as-a-Service-Anbietern (z. B. salesforce.com) auch sog. Platform-as-a-Service- (z. B. Amazon) und Web-Services-Anbieter, welche mit sogenannten „Application Programming Interfaces" die Nutzung unterschiedlicher Funktionalitäten über das Internet ermöglichen (z. B. Yahoo! Maps oder Flickr).

Da Cloud Computing Daten und Infrastruktur voneinander trennt, verliert der Anwender die Kontrolle über die Applikation sowie den Speicher- und Absicherungsort der Daten. Dadurch entstehen neue Risiken hinsichtlich Compliance, Datenschutz, Verfügbarkeit sowie Backup und Recovery. Mögliche Compliance-Probleme entstehen beispielsweise in der EU durch die Vorschrift, private Daten (zu denen auch E-Mails gezählt werden) in einem Datencenter innerhalb der EU zu speichern.

Da die Absicherung der Anwendungsdaten beim Transfer zwischen lokalem Client und entferntem Server oft noch nicht ausreichend gewährleistet werden kann, stellen Sicherheitsrisiken weiterhin eine Barriere beim Eintritt in

---

[48] CIO, Gartner erwartet starke IT-Regulierung, 2009

[49] Koalitionsvertrag zwischen der CDU, CSU und FDP für die 17. Legislaturperiode, 2009

[50] Cloud Computing steht für einen Pool aus abstrahierter, hochskalierbarer und verwalteter IT-Infrastruktur, die Kundenanwendungen vorhält und ggf. nach Nutzung abgerechnet werden kann

das Cloud Computing dar. Vor dem Hintergrund der signifikanten Kosteneinsparungs- und Effizienzsteigerungspotentiale nutzen derzeit allerdings schon ca. 20% aller Unternehmen Software-as-a-Service-Produkte oder führen einschlägige Pilotprojekte durch.[51] Daneben bietet das Cloud Computing aber auch Sicherheitsvorteile: Durch die Redundanz der Server innerhalb einer Cloud-basierten Infrastruktur kann eine sicherere Betriebsbereitschaft gewährleist werden.

Internet der Dinge

Das „Internet der Dinge" ist eine Bezeichnung für die Vernetzung von Gegenständen des Alltags. Dabei sollen z. B. über die Radio Frequency Identification Technologie (RFID), die bisher nur zur funktechnischen Identifikation von Objekten benutzt wird, Gegenstände zukünftig selbstständig miteinander kommunizieren können. Die Vision auf diesem Gebiet ist ein weltweites System vernetzter und über ein Standard-Kommunikationsprotokoll eindeutig adressierbarer Objekte, die Informationen austauschen können. Die Sicherheitsrisiken in einem solchen System sind enorm, da eine Manipulation Auswirkungen auf die Interaktion physischer Objekte hätte.[52]

Sicherheit in drahtlosen Sensorennetzen

Ein drahtloses Sensorennetz besteht aus einer Reihe von Sensoren, die über einen Funkkanal miteinander kommunizieren. Diese Netze kommen zunehmend zum Einsatz, da sie geringere Kosten verursachen und flexibler einsetzbar sind als verkabelte Sensorennetzwerke. Einsatzgebiete sind u. a. Logistik und Verkehrsüberwachung, der Katastrophenschutz oder die Überwachung von Gebäuden. Angesichts des vermehrten Einsatzes dieser Sensorennetzwerke hat sich die IT-Sicherheitsbranche auch mit deren Sicherheit zu beschäftigen. Besondere Herausforderungen stellen hier die beschränkten Hardware- und Energieressourcen sowie die Manipulationsgefahr durch die Funkverbindung dar.[53]

[51] Forrester, How Secure is Your Cloud?, 2009
[52] BSI, Die Lage der IT-Sicherheit in Deutschland, 2009
[53] BSI, Die Lage der IT-Sicherheit in Deutschland, 2009

Biometrie in Kombination mit Kryptographie

Die Biometrie ist ein wichtiges zukünftiges Einsatzgebiet von Passwörtern und Zugangsberechtigungssystemen. Die Forschung sucht derzeit nach einem Verschlüsselungsverfahren, welches die Rekonstruktion eines biometrischen Merkmals unmöglich macht.

Quantencomputerresistente Kryptoverfahren

Mit neuartigen Computern, die voraussichtlich eine deutlich vergrößerte Rechenleistung haben, könnten zurzeit verwendete kryptographische Algorithmen gebrochen werden. Daher wird fortlaufend an neuartigen kryptographischen Algorithmen gearbeitet.

4.4.5 Der Einfluss der Wirtschaftskrise auf den IT-Sicherheitsmarkt

Die Auswirkungen der gegenwärtigen Wirtschaftskrise auf die Nachfrage nach IT-Sicherheitsprodukten und -dienstleistungen sind moderat. Umfragen zufolge ist die IT-Sicherheit ein Bereich, in dem die Unternehmen trotz des Kostendrucks keine großen Einsparungen planen.[54] Lediglich etwa 10% aller Betriebe weltweit planen eine Kürzung des IT-Sicherheitsbudgets, während mit ca. 60% die Mehrheit von einem unveränderten Investitionsniveau ausgeht. Die verbleibenden 30% planen für 2009 sogar eine Ausweitung des Investitionsniveaus.[55] Eine Vernachlässigung des Basisschutzes vor IT-Sicherheitsbedrohungen oder von Compliance-Vorgaben können sich die Unternehmen heute, auch während eines wirtschaftlichen Abschwungs, nicht mehr leisten.[56] Dennoch verliert die IT-Sicherheit vor dem Hintergrund notwendiger Sparmaßnahmen bei einigen Unternehmen den Status der Top-Priorität. Dort stehen nun wieder die IT-Kernprozesse wie die ERP-Systeme (Einführung, Updates, Harmonisierung) sowie das IT-Infrastrukturmanagement im Vordergrund.[57] Interviews mit deutschen Anbieterunternehmen haben diesen Trend nur zum Teil bestätigt, unter anderem bedingt durch das IT-Investitionsprogramm der Bundesregierung, dass mit Beschaffungen von IT-Sicherheit in Höhe von über 200 Mio. Euro in 2009 einen spürbaren Nachfrageimpuls gesetzt hat. Von einigen Unternehmen wird die Wirt-

[54] IDC, Worldwide IT Security Software, Hardware, and Services, 2009
[55] Forrester, The Enterprise IT Security Buyer Profile, 2009
[56] Computerwoche, Sicher trotz Krise, 2009
[57] Capgemini, IT-Trends, 2009

schaftskrise auch als Chance zur Stärkung der eigenen Position am Markt und zur Gewinnung von Marktanteilen gesehen.[58]

[58] Interviews mit Anbieterfirmen, 2009

4.5 Beurteilung der Entwicklung nach Marktsegmenten für die Jahre 2010–2015

Der weltweite Markt für IT-Sicherheit lässt sich grob zu je 50% in Dienstleistungen und Produkte aufteilen (vgl. Abschnitt 4.2.1). Innerhalb des Produktsegments kann hinsichtlich der Marktgröße und des prognostizierten Wachstums der Untersegmente zwischen zwei Kategorien unterschieden werden:

1. Die **„traditionellen Segmente"** Netzwerksicherheit und Endgerätesicherheit haben ein hohes Umsatzvolumen (ca. 4–5 Mrd. Euro), weisen jedoch in den nächsten Jahren voraussichtlich ein geringeres Wachstum (8–10%) auf.

2. Die **„neuen Wachstumssegmente"** Datensicherheit, Nachrichtensicherheit und Web-Sicherheit sind durch ein (bisher noch) geringeres Umsatzvolumen (1–2,5 Mrd. Euro) aber ein höheres prognostiziertes Wachstum (11–16%) gekennzeichnet.

Für das Segment der Identitäts- und Zugriffsverwaltungen gehen die Wachstumsprognosen stark auseinander (z. B. für 2009: Forrester 21%, IDC 9%). Dennoch kann es eher der zweiten Gruppe zugeordnet werden.

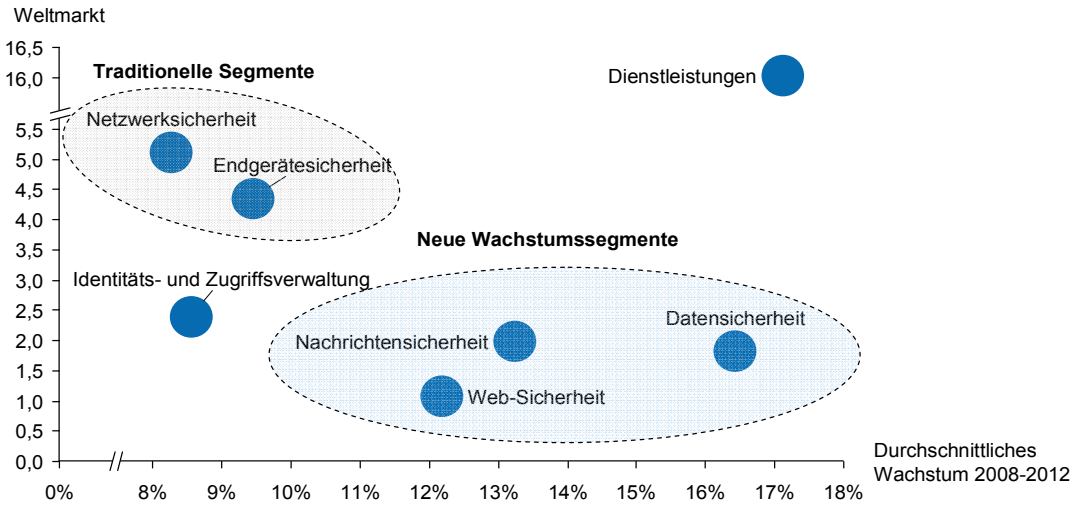


Abbildung 21: Größe und Wachstum der Marktsegmente im Bereich der IT-Sicherheit (weltweit) 2008 und prognostiziert bis 2012 (in Mrd. Euro)[59]

[59] IDC, Worldwide IT Security Software, Hardware, and Services, 2009

Hinsichtlich der Darstellung und Analyse der einzelnen Segmente kann aus den in Abschnitt 4.2.4 beschriebenen Gründen weitgehend auf die Daten der Markteinschätzung von IDC zurückgegriffen werden.

Die derzeitige Größe der einzelnen Marktsegmente in Deutschland sowie die Prognose bis 2012 ist in Abbildung 22 zusammengefasst.

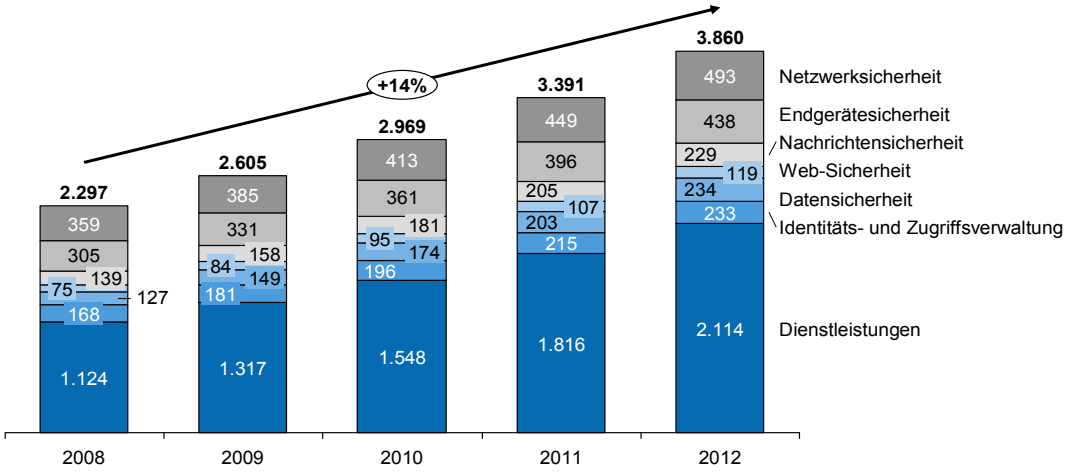


Abbildung 22: Umsätze nach Segmenten im deutschen IT-Sicherheitsmarkt 2008 und prognostiziert bis 2012 (in Mrd. Euro)[60]

In den einzelnen Segmenten sind weltweit folgende Entwicklungen zu beobachten:

4.5.1 Netzwerksicherheit

Mit weltweit ca. 5,1 Mrd. Euro ist die Netzwerksicherheit das größte Produktsegment im Bereich der IT-Sicherheit. Allerdings wird aufgrund der Ausweitung der Netzwerkaußengrenzen und dem daraus folgenden Fokus auf die Datensicherheit (vgl. Abschnitt 4.4) für dieses Segment in den nächsten Jahren mit durchschnittlich 8% ein geringeres Wachstum erwartet als in anderen Segmenten.[61] Wachstumstreiber sind hauptsächlich Multifunktions-Appliances sowie die Weiterverbreitung der traditionellen Netzwerkschutzfunktionen (Firewalls etc.).[62] Dagegen wird z. B. im Bereich Intrusion Detecti-

[60] IDC, Worldwide IT Security Software, Hardware, and Services, 2009
[61] IDC, Worldwide IT Security Software, Hardware, and Services, 2009
[62] Forrester, Market Overview IT Security, 2009

on weniger investiert, da der Entwicklungsaufwand dieser Produkte meist zu hoch ist.[63]

4.5.2 Endgerätesicherheit

Mit ca. 4,4 Mrd. Euro Gesamtumsatz ist die Endgerätesicherheit das zweitgrößte Produktsegment. Ein wesentlicher Teil der Umsätze mit Privathaushalten wird in diesem Segment erzielt. Hier steigt insbesondere die Nachfrage nach Gesamtlösungen (wie z. B. die Kombination von Desktop-Antivirus, Antispyware und Firewall) weiter. Die Nachfrage vonseiten der Unternehmen wächst insbesondere für Endgerätesicherheitsprodukte, die im Zusammenhang mit dem Schutz von Daten stehen, sowie für Produkte zum Schutz von mobilen Endgeräten.[64] Insgesamt wird in diesem Segment, ähnlich wie im Bereich Netzwerksicherheit, ein moderateres Wachstum erwartet. Forrester geht von einem Wachstum von lediglich 2% aus, da der Markt schon weitgehend gesättigt sei. IDC ist mit 9% deutlich optimistischer.[65]

4.5.3 Datensicherheit

Die Datensicherheit gehört mit einem Gesamtumsatz von 1,8 Mrd. Euro zu den kleineren Segmenten des Marktes für IT-Sicherheit, ist aber das am stärksten wachsende Produktsegment. Wie im Abschnitt 4.4.3 beschrieben, erscheint der Fokus auf den Datenschutz zunehmend effektiver als der Schutz der Systeme bzw. Geräte. Daher wird in diesem Segment ein hohes Umsatzwachstum von jährlich 16% erwartet.[66]

Die wachsende Anzahl von Datenschutz- und Compliance-Gesetzen zwingt viele Unternehmen zur Einführung von Produkten, die nicht nur die Einhaltung der Gesetze gewährleisten, sondern auch Auswertungen für eine interne und externe Kontrolle ermöglichen. Wie im Abschnitt 4.4.3 beschrieben, haben viele Unternehmen hier noch Nachholbedarf. Darüber hinaus wird erwartet, dass die Segmente Data Loss Prevention und Digital Rights Management weiter zusammenwachsen. Der Bereich Digital Rights Management wird insbesondere auch für Unternehmen außerhalb der Medienindustrie relevant.

---

[63] Interviews mit Anbieterunternehmen
[64] Griephan Global Security, Strategische Industrie IT, 2009
[65] IDC, Worldwide IT Security Software, Hardware, and Services, 2009
[66] IDC, Worldwide IT Security Software, Hardware, and Services, 2009

4.5.4 Identitäts- und Zugriffsverwaltung

Da die Identitäts- und Zugriffsverwaltung insbesondere im Zusammenhang mit Compliance-Anforderungen zunehmend an Relevanz gewinnt, ist auch in diesem Segment weiterhin mit einem starken Nachfragewachstum zu rechnen, gerade auch vonseiten kleiner und mittelständischer Unternehmen. Besonderes Wachstumspotenzial haben u. a. Produkte im Bereich Privileged User Password Management.[67] Insgesamt werden im Bereich Identitäts- und Zugriffsverwaltung weltweit ca. 2,3 Mrd. Euro umgesetzt.

4.5.5 Web-Sicherheit

Die Nachfrage nach Web-Sicherheitsprodukten ist durch die zunehmende Raffiniertheit webbasierter Angriffe und der wachsenden Zahl von Web-2.0-Applikationen mit zusätzlichem Bedrohungspotenzial ungebrochen.[68] Ein Wachstumsbereich sind Web Security Hosted Services (z. B. zentralisierte Hosted Malware Protection und Web-Filter) die als Plattform zunehmend attraktiver werden. Mit einem Gesamtumsatz von rund 1,0 Mrd. Euro ist die Web-Sicherheit das kleinste Untersegment. Das prognostizierte Wachstum liegt bei 12%.

4.5.6 Nachrichtensicherheit

Mit einem Gesamtumsatz von 2,0 Mrd. Euro gehört auch die Nachrichtensicherheit zu den kleineren Segmenten. Hier wird ein durchschnittliches Wachstum von 13% erwartet. Wachstumstreiber sind u. a. sog. Hybrid-Modelle, welche virtuelle Anwendungen und Hosted Services (wie z. B. SaaS) mit klassischen hardwarebasierten Applikationen kombinieren. Damit wird für die Kunden eine größtmögliche Flexibilität und Sicherheit gewährleistet.[69] Insbesondere die Anzahl der Firmen, welche Hosted Messaging Services in Anspruch nehmen, steigt.

4.5.7 Dienstleistungen

Wie bereits in Abschnitt 4.2 beschrieben, sind die Dienstleistungen das am stärksten wachsende Segment im IT-Sicherheitsbereich. Wesentliche Wachstumstreiber sind die zunehmende Komplexität der IT-Sicherheit, die Ver-

---

[67] Bezeichnung für die Verwaltung und den Schutz von Passwörtern mit Sonderzugriffsrechten (Administratoren etc.)
[68] IDC, Worldwide IT Security Software, Hardware, and Services, 2009
[69] IDC, The Latest in "Hybrids": Deployment Models for Email Security, 2009

knüpfung von Dienstleistungen mit Produkten, die Integration unterschiedlicher Sicherheitsprodukte sowie die zunehmende Anzahl von Schulungen zur Verbesserung des Sicherheitsverständnisses der Mitarbeiter. Dienstleistungen, die im Zusammenhang mit diesen Entwicklungen stehen, haben ein signifikantes Wachstumspotential und können als die derzeit attraktivsten (Unter-)Segmente innerhalb des IT-Sicherheitsmarktes angesehen werden.

Auch die Nachfrage nach umfassenden Managed Security Services steigt vor dem Hintergrund der o. g. Entwicklungen. Dabei sind Dienstleistungen, welche die unterschiedlichen Teilaspekte der IT-Sicherheit integrieren und somit auch die Effizienz des Gesamtsystems verbessern können, besonders gefragt.

4.6 Betrachtung von Regionen mit besonders hohen Wachstumserwartungen

Die Entwicklung der Nachfrage für IT-Sicherheit hängt in hohem Maße von den Umsätzen des gesamten IT-Marktes ab. Darüber hinaus besteht auch zwischen dem Wirtschaftswachstum im Allgemeinen und den Zuwächsen in der IT-Branche eine hohe Korrelation. Daher sind die Märkte mit den höchsten Wachstumserwartungen für IT-Sicherheit diejenigen, wo auch das höchste Wirtschaftswachstum erwartet wird. Dazu gehören die sog. BRIC-Länder (Brasilien, Russland, Indien und China) sowie einige Länder im südostasiatischen Raum, im Mittleren Osten und in Osteuropa. Die positiven Wachstumsaussichten in diesen Ländern wurden auch schon in der 2004 durchgeführten Studie für das Bundesministerium für Wirtschaft und Arbeit neben strategisch/ politischen Entscheidungen als eine sehr wichtige Entscheidungsgundlage für einen geplanten Markteintritt herausgearbeitet.[70] In der folgenden Abbildung sind diese Länder geordnet nach der Größe des IT-Marktes dargestellt.

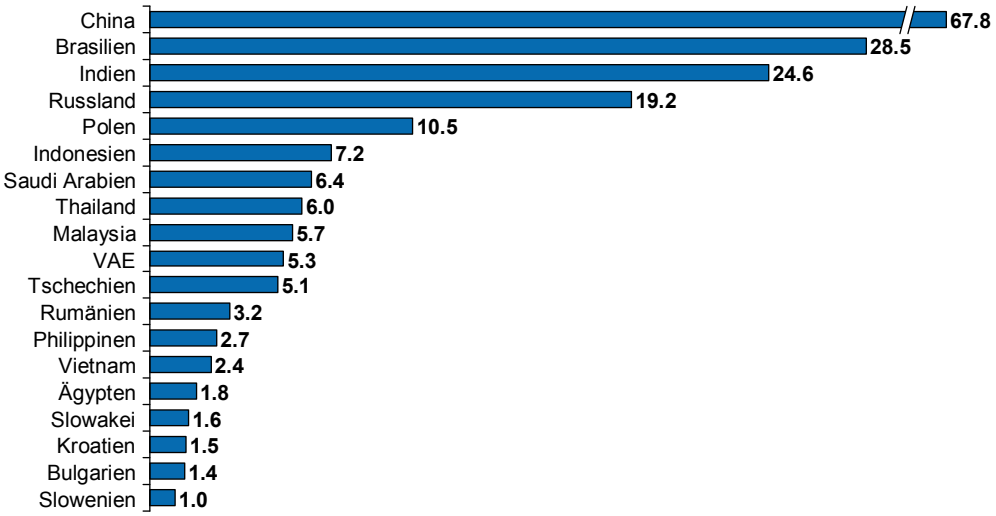


Abbildung 23: IT-Marktgröße 2008 internationale Märkte (in Mrd. USD)[71]

[70] Booz & Company/Secartis, Exportchancen der deutschen IT-Sicherheits- und Kryptowirtschaft, Studie für das Bundesministerium für Wirtschaft und Arbeit, 2004

[71] IDC, 2009

4.6.1 BRIC-Länder

Unter den BRIC-Ländern ist China mit 1,4 Mrd. US-Dollar der mit Abstand größte Markt für IT-Sicherheit, auf dem die Umsätze u. a. durch die Expansion der einheimischen IT-Sicherheitsfirmen wie Rising oder Kingsoft allein im Jahre 2008 um ca. 40% gesteigert wurden. Analysten erwarten auch in den nächsten Jahren weiterhin ein durchschnittliches Wachstum von ca. 30%. Das Umsatzvolumen für IT Sicherheit steigt damit auf 2,8 Mrd. USD in 2012.[72]

Im gesamten asiatisch-pazifischen Raum sind die größten Anbieter Symantec, Trend Micro, McAfee, EMC und IBM: Zusammen vereinigen sie einen Marktanteil von ca. 50% auf sich. Dieser Anteil verringert sich jedoch zurzeit zugunsten von kleineren Spezialanbietern und neuen Unternehmen am Markt, was die Dynamik und die Chancen in der Region unterstreicht.[73]

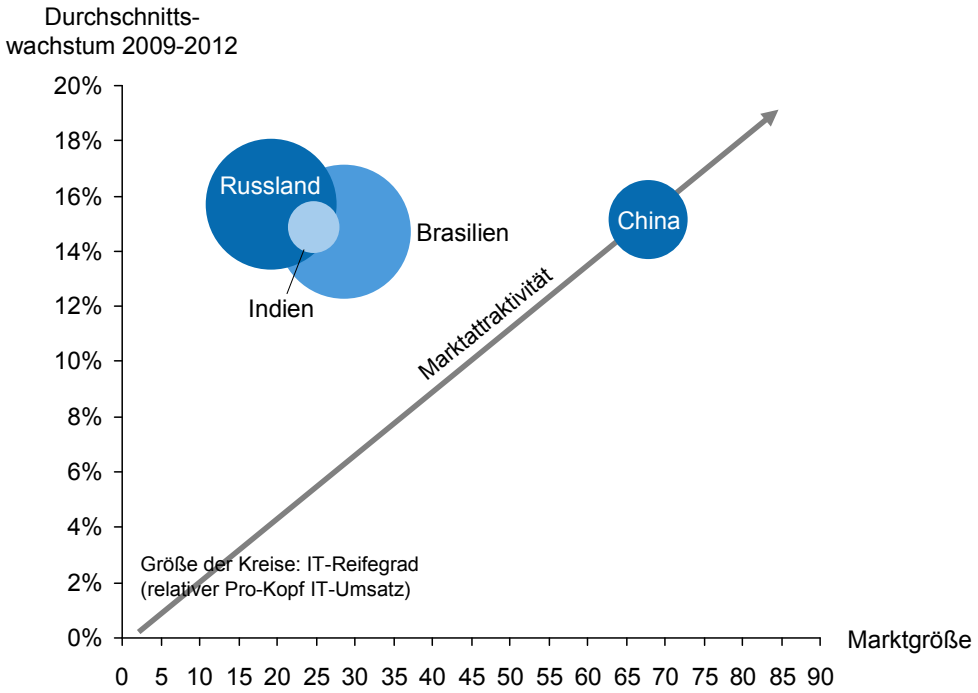


Abbildung 24: IT-Marktgröße 2008 und Wachstumsprognose bis 2012 in den BRIC-Ländern (in Mrd. USD)[74]

[72] Asiainfo, Presentation to Investors, 2009
[73] Gartner, HK security market growth lower than APAC average, 2009
[74] IDC Forecast, 2009

In Brasilien, Russland und Indien wird in den nächsten Jahren ebenfalls mit einem hohen Wachstum gerechnet. Die Märkte sind jedoch deutlich kleiner (die Größe aller drei Märkte zusammen entspricht etwa der Größe des chinesischen Marktes). Das Umsatzwachstum im gesamten IT-Markt, von dessen Entwicklung die Nachfrage für IT-Sicherheit abhängt, wird in Russland, Brasilien und Indien ähnlich wie auch in China auf jährlich 14–16% geschätzt[75] (vgl. Abbildung 24). Ein großer Unterschied zwischen den Märkten besteht hinsichtlich des IT-Reifegrades, als dessen Indikator der IT-Umsatz pro Kopf gilt. Dieser ist in Brasilien dreimal so hoch wie in China und siebenmal so hoch wie in Indien.

4.6.2 Südost-Asien- Mittlerer Osten

Weitere Wachstumsmärkte sind die südostasiatischen Länder Vietnam, Philippinen, Malaysia, Indonesien, Thailand sowie im arabischen Raum Ägypten, die Vereinigten Arabischen Emirate und Saudi-Arabien. Im Vergleich zu den BRIC-Ländern sind diese allerdings nicht nur deutlich kleiner, sondern wachsen mit 7–14% auch langsamer.

Der am weitesten entwickelte IT-Markt innerhalb dieser Gruppe sind (mit großem Abstand) die Vereinigten Arabischen Emirate, gefolgt von Saudi-Arabien und Malaysia. In den Ländern Vietnam, Philippinen, Indonesien und Ägypten ist der Entwicklungsstand des IT-Marktes deutlich niedriger und vergleichbar mit dem Niveau von China und Indien.

[75] IDC Forecast, 2009

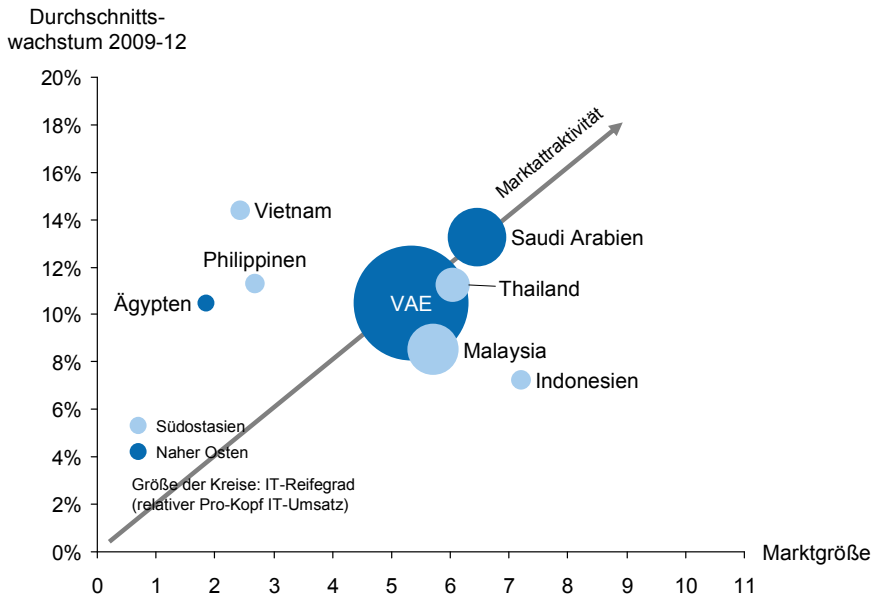


Abbildung 25: IT-Marktgröße 2008 und Wachstumsprognose bis 2012 für Südostasien und den Mittleren Osten (in Mrd. USD)[76]

4.6.3 Osteuropa

Im osteuropäischen Markt sind Rumänien und Bulgarien, für welche mit ca. 18% ein sehr hohes jährliches Wachstum prognostiziert wird, von den Ländern Kroatien, Slowakei, Slowenien, Tschechische Republik und Polen zu unterscheiden. In diesen Ländern wächst der IT-Markt mit jährlich 7–9% im Vergleich nur halb so schnell. In der Summe wird für Osteuropa speziell für den IT-Sicherheitsmarkt ein jährliches Wachstum von 17% prognostiziert.[77] Der Sicherheitsmarkt wächst demnach annähernd doppelt so schnell wie der IT- Gesamtmarkt. Die IT-Umsätze pro Kopf sind in Osteuropa relativ homogen und durchgehend höher als in den BRIC-Staaten sowie (bis auf Malaysia) höher als in allen südostasiatischen Ländern.

[76] IDC, Forecast, 2009

[77] IDC, The European Network and Information Security Market, 2009

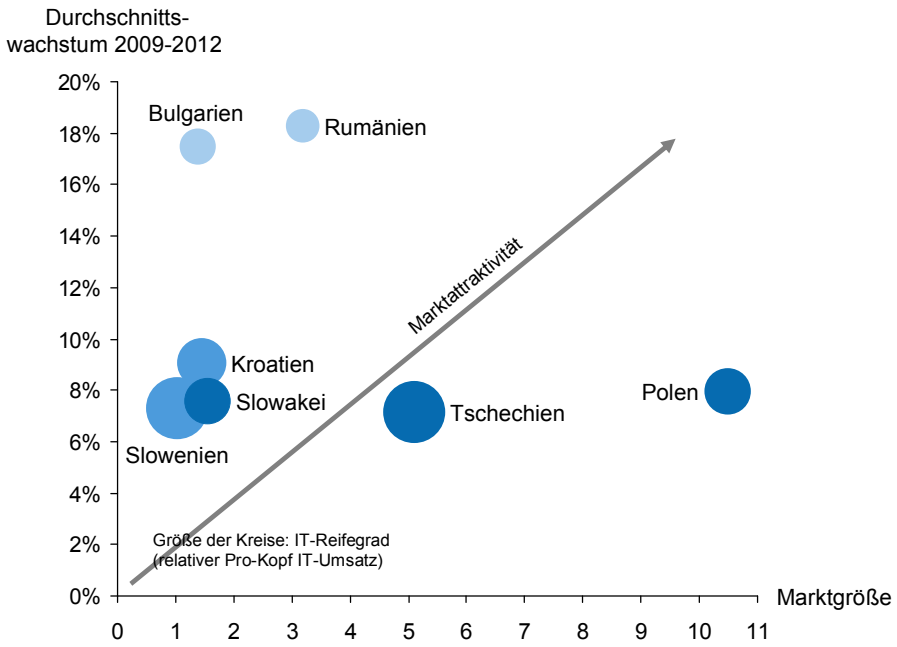


Abbildung 26: IT-Marktgröße 2008 und Wachstumsprognose bis 2012 für Osteuropa (in Mrd. USD)[78]

4.7 Relevante Wettbewerbsfaktoren

Zu den relevanten Wettbewerbsfaktoren zählen sowohl die spezifischen Eigenschaften des Anbieters als auch die Eigenschaften des Produkts bzw. der Dienstleistung. Hinsichtlich der Anbietereigenschaften sind im Bereich der IT-Sicherheit u. a. die plausible Darstellung des Nutzens für den Kunden, die Herstellung von Glaubwürdigkeit bzw. Kundenvertrauen, die Sicherstellung einer langfristigen Kundenbetreuung sowie ein weitreichendes Vertriebspartnernetz wichtige Wettbewerbsfaktoren. Auf der Produktseite sind vor allem Flexibilität bzw. Kompatibilität, die Zukunftsfähigkeit/ Standardisierung der Produkte sowie eine einfache Implementierung und Integrationsfähigkeit relevant.[79]

[78] IDC, Forecast, 2009

[79] Die Zusammenstellung dieser Wettbewerbsfaktoren basiert im Wesentlichen auf Interviews mit Anbieter- und Anwenderunternehmen sowie Experten

4.7.1 Plausibilisierung des Nutzens für den Kunden

Compliance-Anforderungen

IT-Sicherheit ist zunehmend nicht nur als Präventivmaßnahme, sondern auch im Zusammenhang mit der Erfüllung von Compliance-Anforderungen relevant. In diesem Zusammenhang haben Anbieter einen Wettbewerbsvorteil, welche die Compliance-Anforderungen für ihre Kunden sowie die Folgen bei möglichen Verstößen dagegen aufzeigen und passende – oft länderspezifische - Lösungen dazu anbieten.

Zuordnung zu direkten Bedrohungen

Die Möglichkeit, die Produkte direkt den unterschiedlichen Bedrohungsszenarien zuzuordnen, und damit die Herstellung einer hohen Transparenz über den spezifischen Nutzen eines Produktes bzw. einer Dienstleistung ist als Wettbewerbsfaktor relevant.

Quantifizierbarkeit des Return on Security Investment (ROSI)

Da IT-Sicherheitslösungen in der Regel die Funktion der Abwendung potenzieller Bedrohungen der IT haben, ist ihr Wert oftmals nur schwer quantifizierbar. Daher müssen Anbieter explizit aufzeigen, inwiefern die angebotene Sicherheitslösung – unter Berücksichtigung der Kosten und der Wahrscheinlichkeit eines potenziellen Schadens – für das Unternehmen wirtschaftlich sinnvoll ist. Die Investition muss dabei z. B. einen ausreichend hohen Return on Security Investment (ROSI) aufweisen. Eine Quantifizierung der Vorteilhaftigkeit des Produktes durch ROSI oder andere relevante Kennzahlen ist insbesondere auch für die Unterstützung des IT-Budgetverantwortlichen bei der internen Rechtfertigung der Investition hilfreich.

Bestandteil des Geschäftsmodells

Zukünftig wird IT für viele Unternehmen zunehmend vom Hilfsmittel zum integralen Bestandteil des Geschäftsmodells (engl. business enabler). Im Zusammenhang mit dieser Entwicklung verändern sich die Prioritäten und Perspektiven auch für die IT-Sicherheit. Daher wird die Erweiterung der Funktion von IT-Sicherheit vom reinen Schutz von Ressourcen hin zur Unterstützung von neuen Business-Modellen und -Prozessen durch die Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und damit Vertrauenswürdigkeit zukünftig zu einem wichtigen Wettbewerbsfaktor: Sicherheit muss nicht mehr als ein Problem angesehen werden, welches es zu lösen gilt,

sondern kann einen entwicklungsfördernden Einfluss auf das Unternehmen haben.

4.7.2 Erleichterung der Implementierung und Integration

Für viele Unternehmen ist die Implementierung eine entscheidende Hürde bei der Einführung eines Sicherheitssystems, vor allem, wo das Sicherheitsprodukt nicht als Teil einer integrierten Lösung angeboten wird. Vor diesem Hintergrund ist es entscheidend, die Sicherheitslösung mit einem auf die bestehenden IT-Systeme und IT-Managementtools und -prozesse zugeschnittenen Integrationsplan zu verbinden. Dazu gehört auch die Gewährleistung der Konformität des Produktes mit den einschlägigen IT-Sicherheitsstandards einerseits (z.B. ISO 17001) und offenen Industriestandards andererseits, z.B. des World Wide Web Consortiums (W3C) oder des Joint Technical Committee der ISO und IEC (ISO/IEC JTC 1) zur Sicherstellung der Interoperabilität des Produkts. Zur Überwindung dieser Hürde, bieten sich den deutschen Anbietern in Anbetracht ihrer geringen Größe und ihrer Einzellösungen Kooperationen mit Systemintegratoren bzw. Lösungsanbietern an.

4.7.3 Flexibilität / Zukunftssicherheit

Um auch in einem Umfeld von sich ändernden IT-Systemen und Unternehmensstrukturen längerfristig einsatzfähig zu sein, muss ein IT-Sicherheitssystem ein hohes Maß an Flexibilität aufweisen. Zudem sollte die Kompatibilität mit zukünftigen Technologien wie z. B. dem IPv6-Format sowie die Internationalisierbarkeit der Sicherheitslösung gewährleistet sein.

4.7.4 Glaubwürdigkeit / Kundenbeziehung

Das Vertrauen in den Anbieter ist eine wichtige Komponente beim Vertrieb eines IT-Sicherheitsprodukts. Oftmals ist daher ein längerer Verkaufs- und Vertrauensbildungsprozess notwendig, bevor es zum Vertragsabschluss kommt. Dabei spielt auch eine neutrale Bestätigung von Qualitätsstandards, wie beispielsweise eine Zertifizierung durch akkreditierte Stellen oder Referenzen in der deutschen Verwaltung, eine wichtige Rolle. Im Hochsicherheitsbereich ist allerdings die Nationalität bzw. Neutralität des Anbieters ein übergeordneter Gesichtspunkt.

4.7.5 Spezialisiertes Angebotsspektrum

Die Anforderungen an IT-Sicherheitslösungen sind branchenabhängig. Im Finanzsektor beispielsweise sind die Anforderungen ungleich komplexer und von anderer Natur als in einem Produktionsbetrieb. Spezialisierte Anbieter kennen die spezifischen Sicherheitsprobleme ihrer Kunden und können individualisierte Lösungen anstelle eines Standardproduktes anbieten.

Angesichts der Dynamik des IT-Sicherheitsmarktes ist die Fähigkeit, schnell auf Markttrends zu reagieren sowie passgenaue Lösungen für Wachstumsfelder zu entwickeln (wie aktuell z. B. integrierte Lösungen für Netzwerk- und Datensicherheit), ein relevanter Wettbewerbsfaktor.

4.7.6 Sicherstellung einer langfristigen Kundenbetreuung

Die IT-Sicherheit eines Unternehmens kann nicht durch eine punktuelle Investition in ein Produkt gewährleistet werden, sondern nur durch die Aufrechterhaltung eines kontinuierlichen Wartungs-, Anpassungs-, Aktualisierungs- und Weiterentwicklungsprozesses. Vor diesem Hintergrund ist auch die Größe eines Anbieters bzw. die damit verbundene Fähigkeit, wirtschaftliche Zyklen zu überstehen (oft auch durch den erleichterten Zugang zu Kapital), ein relevanter Wettbewerbsfaktor.

4.7.7 Vertriebspartnernetz / Kooperationen

Die deutschen IT-Sicherheitsanbieter haben aufgrund ihrer KMU-Struktur keinen Zugriff auf globale Vertriebs- und Servicenetze, die eine Betreuung rund um die Uhr ermöglichen, die insbesondere für global tätige Kunden von großer Bedeutung ist.[80] Sie sind daher auf eine Zusammenarbeit mit inländischen oder ausländischen Kooperationspartnern angewiesen, die über ein Vertriebsnetz im entsprechenden Auslandsmarkt verfügen. Allerdings ist auch im Inland ein weitreichendes Vertriebspartner-Netz oft der entscheidende Faktor für eine erfolgreiche Vermarktung. In diesem Zusammenhang sind verschiedene Arten der vertrieblichen Zusammenarbeit verbreitet:

- Reine **Distributionspartnerschaften**, bei denen Produkte über das Vertriebsnetz des Partners vertrieben werden.

[80] "The European Network and Information Security Market", IDC EMEA, Schlussbericht, April 2009

- Zusammenarbeit mit **Systemintegratoren bzw. Lösungsanbietern,** die auf der Basis der Produkte passgenaue Lösungen entwickeln und diese in Unternehmen implementieren.

Tendenziell im Unterschied zu den deutschen Anbietern haben US-amerikanische IT-Sicherheitshersteller den Weg über die Zusammenarbeit mit Lösungsanbietern gesucht und sich die Nähe zur großen amerikanischen IKT-Industrie zu Nutze gemacht. Beispielsweise hat Symantec OEM-Partnerschaften für Sicherheitssoftware mit einer Reihe namhafter PC-Hersteller geschlossen mit der Folge, dass auf einem Großteil der PCs dieser Hersteller (insbesondere im Privatkundenbereich) eine für einige Zeit kostenlose Version der Symantec-Software vorinstalliert ist. Der amerikanische IT-Sicherheitsanbieter McAfee hat eine ähnliche Partnerschaft mit Dell geschlossen.

5 Die Anbieter der deutschen IT-Sicherheitsbranche

Die Struktur der deutschen Anbieterlandschaft im Bereich der IT-Sicherheit ist recht heterogen, sowohl hinsichtlich der Größe und Organisation der Unternehmen als auch hinsichtlich ihres Produktportfolios. Die Anbieterseite wird daher in diesem Abschnitt zunächst in einer Gesamtsicht dargestellt und einer Einordnung unterzogen (Abschnitt 5.1). Um auch strukturelle Entwicklungen in der Anbieterlandschaft aufzuzeigen, werden aktuelle Ereignisse und Angebotstrends untersucht (Abschnitt 5.2). In einer Detailbetrachtung werden ausgewählte deutsche Kernanbieter exemplarisch im Profil dargestellt (Abschnitt 5.3) sowie einige globale Anbieter mit signifikanter Marktposition in Deutschland skizziert (Abschnitt 5.4).

5.1 Übersicht über die Anbieter für IT-Sicherheit in Deutschland

Der deutsche Markt für IT-Sicherheit ist stark fragmentiert. Für die Analyse der deutschen Anbieter für IT-Sicherheit wurden im Rahmen dieser Studie 135 Unternehmen ausgewählt, die aufgrund ihrer Marktabdeckung und auch in ihrer Struktur die Fragmentierung des Marktes reflektieren. Innerhalb dieser Gruppe wurde für 18 Unternehmen eine Detailanalyse vorgenommen (vgl. dazu Abschnitt 5.3).

Unser Sample besteht zu ca. 80% aus kleinen, spezialisierten Anbietern mit unter 50 Mitarbeitern sowie zu je ca. 10% aus Unternehmen, die 50–200 bzw. über 200 Mitarbeiter beschäftigen. IT-Sicherheit wird von vielen Unternehmen auch im Zusammenhang mit anderen IT- oder Sicherheitsdienstleistungen angeboten. (Für die Einteilung in Gruppen nach der Unternehmensgröße wurden hierbei nur die Mitarbeiter im Geschäftssegment IT-Sicherheit berücksichtigt.) Firmen mit nennenswerten IT-Sicherheitssparten sind z. B. Siemens, T-Systems, Giesecke & Devrient, Rohde & Schwarz oder IABG. Neben den deutschen Anbietern haben auch zahlreiche internationale IT-Sicherheitsanbieter wie Symantec, McAfee oder F-Secure Niederlassungen in Deutschland. Darüber hinaus sind die internationalen IT-Dienstleister (z. B. IBM, Accenture, CSC) auch im Bereich der IT-Sicherheit tätig. Entsprechend dem Fokus der Studie auf die deutsche IT-Sicherheitsbranche sind von den in der Stichprobe vertretenen Unternehmen ca. 75% in deutschem und 25% in ausländischem Mehrheitsbesitz (vgl. hierzu auch die Ausführungen zur Abgrenzung der „deutschen Anbieter“ in Abschnitt 3.2).

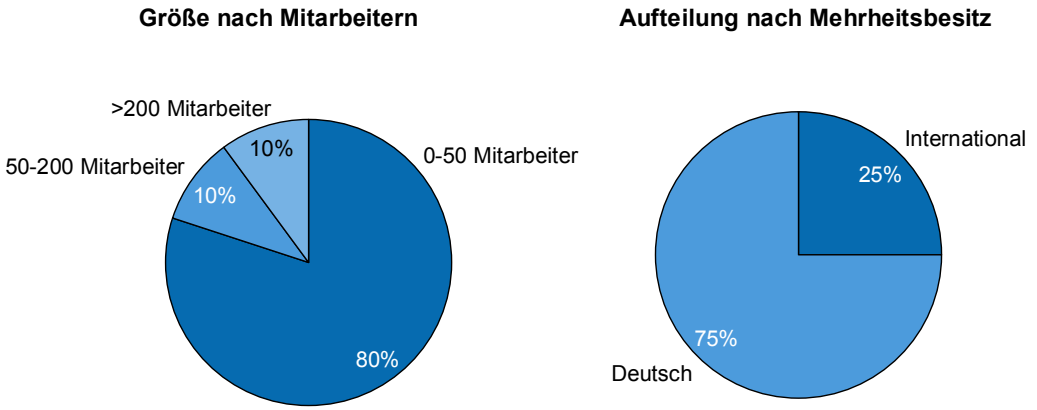


Abbildung 27: Struktur der Anbieter im deutschen IT-Sicherheitsmarkt[81]

Avira und secunet sind dabei die einzigen reinen IT-Sicherheitsanbieter in deutschem Mehrheitsbesitz mit über 200 Mitarbeitern. Beide Unternehmen bieten u. a. Produkte im Bereich der Netzwerksicherheit sowie Beratungsleistungen an. Weitere deutsche Spezialanbieter für IT-Sicherheit in der Größenordnung von 50 bis 200 Mitarbeitern sind u. a. Rohde & Schwarz SIT, GeNUA oder Astaro. In der folgenden Abbildung sind die wichtigsten deutschen und internationalen Anbieter im deutschen IT-Sicherheitsmarkt nach Unternehmensgröße eingeordnet.

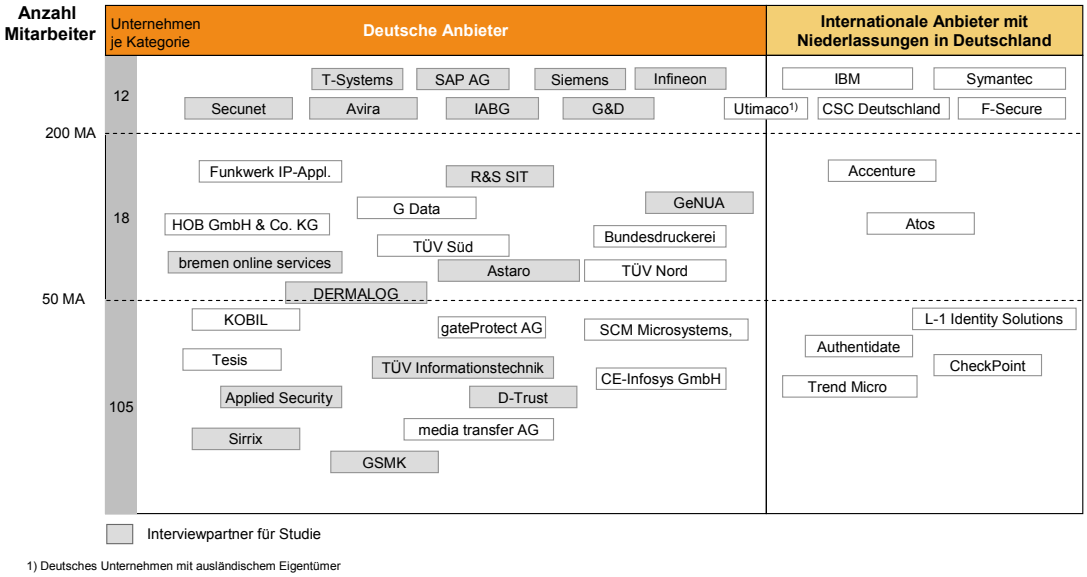


Abbildung 28: IT-Sicherheitsanbieter in Deutschland gruppiert nach Mitarbeiteranzahl[82]

[81] Analyse von 135 Firmen per Desk-Research und Interviews mit ausgewählte Anbietern
[82] Analyse von 135 Firmen per Desk-Research und Interviews mit ausgewählte Anbietern

Obwohl einige deutsche Anbieter jeweils einen großen Teil ihrer Umsätze im Ausland erzielen, hat kein Unternehmen nennenswerte Anteile am weltweiten IT-Sicherheitsmarkt. Unter den 25 weltweit größten IT-Sicherheitsfirmen befindet sich kein deutscher Anbieter.[83]

Im Hinblick auf die geographische Verteilung der IT-Sicherheitsanbieter in Deutschland lässt sich eine Clusterbildung um die Großstädte München und Berlin sowie die Großraumgebiete Rhein-Ruhr, Rhein-Main und Rhein-Neckar ausmachen. Neben der Konzentration in diesen wirtschaftlichen Zentren befinden sich die Firmensitze von IT-Sicherheitsunternehmen häufig in der Nähe von auf IT-Sicherheit spezialisierten Hochschulen und Forschungseinrichtungen wie etwa Karlsruhe, Saarbrücken, Bochum oder Darmstadt. (vgl. Abbildung 29).

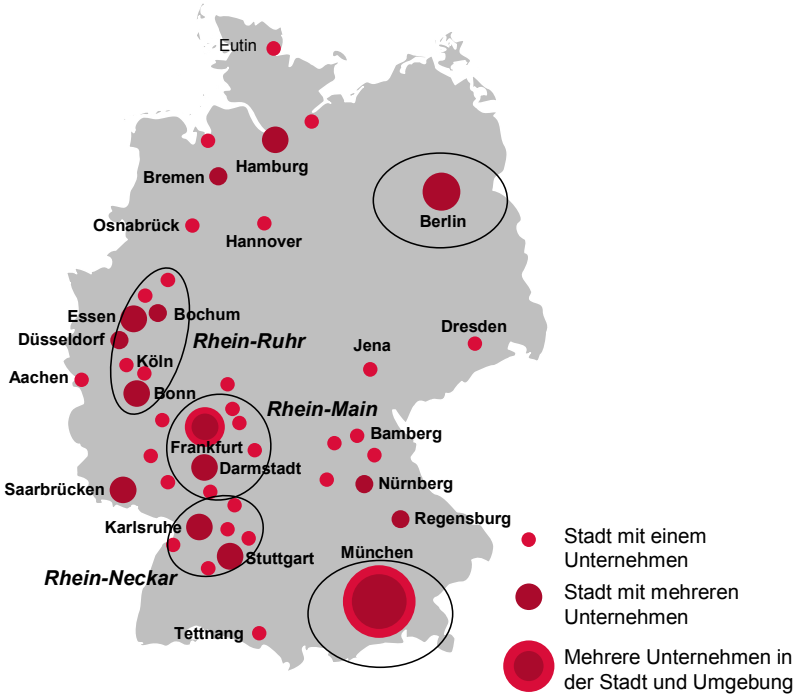


Abbildung 29: Geographische Einordnung der deutschen IT-Sicherheitsunternehmen[84]

[83] IDC, Worldwide IT Security Software, Hardware, and Services, 2009
[84] Booz & Company Analyse

5.2 Aktuelle Ereignisse und Trends auf Anbieterseite

Deutschland hat im Bereich IT-Sicherheit und Kryptographie traditionell eine signifikante Rolle gespielt. Gelegentliche Verweise auf die Chiffriermaschine ENIGMA aus dem Zweiten Weltkrieg führen wohl etwas weit, trotzdem wurden IT-Sicherheit und Kryptographie in Deutschland stets als prestigeträchtig angesehen. Auch im Bereich der Awareness-Bildung gingen von Deutschland wichtige Impulse aus, z. B. durch die von deutschen Firmen entwickelte Verschlüsselungs-Lernsoftware CrypTool. Nachfolgend werden aktuelle Ereignisse und Trends in der Anbieterstruktur betrachtet. Neben institutionellen Veränderungen (z. B. Firmenübernahmen) bei den deutschen und internationalen Anbietern (Abschnitte 5.2.1 und 5.2.2) werden auch Kooperationen und informelle Gruppierungen der Anbieter (Abschnitt 5.2.3) untersucht. Als Referenzpunkt zur Analyse der Veränderungen dient hierbei die Studie „Exportchancen der deutschen IT-Sicherheits- und Kryptowirtschaft" aus dem Jahr 2004, in deren Rahmen bereits eine ausgiebige Anbieteranalyse stattgefunden hat. Im direkten Vergleich zur Situation in 2004[85] ergeben sich einige auffallende Entwicklungen:

- Der Trend von Produktanbietern hin zu Lösungsanbietern hat sich nicht weiter verstärkt. Viele deutsche Produktanbieter haben profitable Nischen gefunden (z. B. nationale Hochsicherheit). Einige konkurrieren auch im Commodity-Bereich (z. B. Antivirus, Netzwerksicherheit für KMU) mit internationalen Anbietern.
- Alleinstellungsmerkmal ist neben der bereits 2004 festgestellten Verknüpfung von Fach-, Prozess- und Produktwissen auch eine profunde technologische Kompetenz, insbesondere in komplexen Produktumfeldern und im Zertifizierungsgeschäft.
- Ein Technologievorsprung ist in ausgewählten Bereichen (z. B. Smartcards, PKI-Lösungen, digitale Signaturen, Hochsicherheitslösungen etc.) weiterhin vorhanden. Allerdings sind die erwarteten Wachstumspotenziale in diesen Segmenten nicht realisiert worden, und einige Leuchtturmprojekte haben sich verzögert (z. B. elektronische Gesundheitskarte).

[85] Booz Studie im Auftrag des BMWi

- Kryptographisches Grundentwicklungspotenzial (z. B. auf der Ebene der Algorithmen) ist in Spezialbereichen immer noch vorhanden (z. B. Verschlüsselung von mobiler Kommunikation, Verschlüsselung von Satellitenkommunikation).
- Die fortschreitende Erosion der IKT-Industrie in Deutschland (z. B. Schließung des Nokia-Werks in Bochum, Einstellung der Mobiltelefonfertigung durch Siemens BenQ, Stilllegung der Chip-Produktion durch Qimonda) erschwert die für das Innovationsklima wichtige Clusterbildung. Wichtige Marktsegmente bzw. Wertschöpfungsstufen sind in Deutschland bereits jetzt nicht mehr vorhanden.
- Der Mangel an qualifizierten Fachkräften und die begrenzte Größe des Binnenmarktes sind unverändert relevante Faktoren für die Anbieter.

5.2.1 Institutionelle Veränderungen in Deutschland

Das Wachstum der Anbieter für IT-Sicherheit in Deutschland gestaltete sich in den letzten Jahren hauptsächlich organisch; ein klarer Konsolidierungstrend war nicht erkennbar. Dennoch hat es in der Vergangenheit, insbesondere im Rahmen der Bestrebung unterschiedliche IT-Sicherheitslösungen integriert anbieten zu können, Unternehmensübernahmen und Zusammenschlüsse gegeben. In diesem Kontext ist vor allem die Übernahme von **Utimaco** durch das britische Unternehmen **Sophos** im Oktober 2008 zu sehen. Mit dieser Übernahme hat die Sophos-Gruppe ihr Angebot an IT-Lösungen für Endgerätesicherheit erweitert, und zwar um Utimacos SafeGuard-Datenschutzprodukte für mittelständische und große Unternehmen sowie dessen Lösungen für E-Mail-Sicherheit, Compliance und Audit. Das kombinierte Unternehmen kann dadurch eine umfassendere Lösung für den Schutz von Kundendaten und Endgeräten vor internen und externen Bedrohungen anbieten. Die Übernahme von Utimaco durch Sophos wurde in der Branche allerdings durchaus kritisch gesehen. Aus der Sicht vieler Interviewpartner sei hiermit „ein“ bzw. „das“ deutsche Vorzeigeunternehmen im Bereich IT-Sicherheit als „deutsches Unternehmen“ verloren gegangen. Entsprechend wird ein Kompetenzverlust und ein Abfluss von Wissen befürchtet. Die Brisanz dieser Transaktion zeigt sich auch darin, dass das Bundeswirtschaftsministerium (BMWi) dem Verkauf nur unter Auflagen zugestimmt hat.[86]

[86] Pressemitteilung der SOPHOS Holdings GmbH

Weiterhin hat im laufenden Jahr (2009) die Schweizer Firma **e.siqia Group** das Hamburger Unternehmen **timeproof Time Signature Systems GmbH** übernommen und damit sein Produkt- und Dienstleistungsportfolio um die Signatur- und Zeitstempel-Serversysteme der timeproof GmbH ergänzt. Dadurch verfügt das Unternehmen über ein vollständiges Angebot von Lösungen im Bereich digitaler Signaturen für Arbeitsplatzanwendungen, und zwar sowohl als Betreibermodell wie als Serverlösung.

Umgekehrt hat der deutsche Antivirus-Spezialist **Avira** durch die Übernahme der schwedischen Firma **Cryptzones** im Jahre 2008 sein Angebotsspektrum um deren Verschlüsselungs- und E-Mail-Sicherheitsprodukte erweitert. Daneben profitiert Avira vom Zugang dieser Firma zu größeren Unternehmen und zum öffentlichen Sektor. Schon 2006 hatte Avira mit der Übernahme von **datapol GmbH** das Produktportfolio um Recovery-Techniken erweitert.

Das Bestreben, IT-Sicherheitsprodukte mit passenden Dienstleistungen zu verbinden, war im Jahr 2006 ein wesentliches Motiv für die Übernahme von **TC-Trust Center**, einem IT-Sicherheitsdienstleister, durch den britischen Identitätsmanagement- und E-Business-Anbieter **GeoTrust.**

Zusammenfassend lässt sich feststellen, dass Firmenübernahmen im deutschen Markt meist von ausländischen Anbietern getätigt werden. Übernahmeaktivitäten innerhalb des deutschen Marktes oder von deutschen Unternehmen auf internationalen Märkten, wie der Kauf von Cryptzones durch Avira, kommen selten vor. Ein Grund hierfür ist insbesondere die schwache Kapitalausstattung der deutschen Anbieter bzw. die begrenzten Möglichkeiten zur Kapitalbeschaffung (z. B. über den Kapitalmarkt oder als Wagniskapital). Obwohl es zu signifikanten Übernahmen gekommen ist, kann nicht von einer breiten Übernahmewelle durch ausländische Investoren gesprochen werden – auch wenn diese Befürchtung bei einigen Anbietern existiert.[87]

5.2.2 Institutionelle Veränderungen auf dem Weltmarkt

Auf internationaler Ebene haben vor allem die großen amerikanischen IT-Sicherheitsanbieter Symantec und McAfee ihr Angebotsspektrum durch Übernahmen erweitert. [88] Beide Unternehmen streben dabei die Position eines

[87] Interviews mit ausgewählten Anbietern im Bereich IT-Sicherheit

[88] The Deal, McAfee, Symantec highlight Web security M&A, 18.05.2009

„One-Stop-Shop"-Anbieters für sämtliche IT-Sicherheitslösungen und breite Kundensegmente an.

Symantec hat in den letzten Jahren durch Zukäufe vor allem die Bereiche Web- und Nachrichtensicherheit, Software as a Service sowie Data Loss Prevention erweitert. In diesem Jahr wurde durch die Übernahme des Websicherheitsanbieters **Mi5 Networks** das Angebot im Bereich Nachrichtensicherheit und Überwachung des Datenverkehrs ergänzt. 2008 wurde das britische Unternehmen **MessageLabs**, ein Anbieter für die Abwicklung von E-Mail-Verkehr und Spezialist für das Herausfiltern von Spam-Mails und anderen schädlichen Inhalten, erworben (für 700 Mio. USD). Die Dienstleistungen von MessageLabs hat Symantec mit eigenen Software-as-a-Service-Angeboten, bestehend aus Online-Backup, Online-Speicher und Remote Access, verbunden. Bereits 2007 hat Symantec durch den Kauf des Sicherheitsspezialisten **Vontu** (für 350 Mio. USD) das Angebotspektrum im Bereich Data Loss Prevention gestärkt. 2004 hatte das Unternehmen (für 13,5 Mrd. USD) den Backup- und Archivierungsspezialisten **Veritas** übernommen und damit eine der größten Übernahmen der Branche vollzogen.

McAfee hat durch Übernahmen neben der Web-Sicherheit auch die Kompetenz in den Bereichen IT-Infrastruktursicherheit, Compliance und Netzwerksicherheit erweitert. Mit der Übernahme des Unternehmens **MX Logic** (für 140 Mio. USD) hat McAfee in diesem Jahr seine Software-as-a-Service-Lösungen für E-Mail on demand, Web-Sicherheit und Archivierung ausgebaut. Daneben wurde ebenfalls 2009 das auf die Kontrolle und den Schutz von installierten Applikationen sowie auf Compliance spezialisierte US-Unternehmen **Solidcore Systems** erworben (für 33 Mio. USD). McAfee stärkt damit u. a. seinen Zugang zum Markt für Endgerätesicherheit, insbesondere bei Verkaufsterminals und mobilen Geräten. McAfee plant ferner, die Compliance-Lösungen von Solidcore, welche die Erfüllung der Vorgaben des Payment Card Industry Data Security Standard (PCI DSS) und des Sarbanes-Oxley Act (SOX) unterstützen, in die Software-Pakete des eigenen Hauses zu integrieren.

Auch mit dem Kauf von **Secure Computing** im Jahre 2008 (für 0,5 Mrd. USD) verfolgt McAfee die Strategie, ein möglichst komplettes Security-Angebot im Netzwerkmarkt anbieten zu können. Mit der Übernahme von **Reconnex** (46 Mio. USD) ist McAfee auch in das Segment Data Loss Prevention eingetreten.

Eine weitere größere Übernahme in der Branche war der Kauf von **RSA** durch **EMC** für 2 Mrd. USD in 2007. Damit ergänzte EMC sein Portfolio an Sicherheitslösungen für die Informationsinfrastruktur um ausgereifte Verschlüsselungstechnologien sowie um Software zur Identitäts- und Zugriffskontrolle.

Durch die o. g. Übernahmen konnten Symantec und McAfee in den letzten Jahren stark wachsen und sich zu internationalen Marktführern entwickeln, die umfassende IT-Sicherheitslösungen über nahezu alle Segmente hinweg anbieten. Dabei haben beide Unternehmen vor allem auch in die Wachstumssegmente Web-, Nachrichten- und Datensicherheit investiert und sind damit zukünftig weiterhin gut im Markt positioniert. Auch in Deutschland sind beide Firmen im Bereich Sicherheitssoftware führend und haben zusammen einen Marktanteil von über 30%.[89]

5.2.3 Strategien deutscher Anbieter im Wettbewerb

Nicht nur auf dem Weltmarkt, sondern auch auf dem deutschen Markt für IT-Sicherheit dominieren die internationalen Anbieter in den Bereichen Software und standardisierte Hardware (siehe Abschnitt 5.4). Anbieter wie Symantec, McAfee, Cisco, IBM, Checkpoint oder Juniper Networks haben bezüglich Kapitalausstattung, Vertriebskraft sowie Skaleneffekten in Entwicklung und Produktion entscheidende Vorteile gegenüber kleinen und mittelständischen deutschen Anbietern. Vor diesem Hintergrund müssen sich deutsche Anbieter mit entsprechenden Strategien im Wettbewerb positionieren.

- Eine Reihe von Anbietern spezialisiert sich auf die **Nische Hochsicherheit** und das Geschäft mit hoheitlichen Auftraggebern. Diese Anbieter machen sich dabei die nationalen Vorbehalte gegenüber internationalen Anbietern zunutze und tätigen einen Großteil ihres Geschäfts mit der öffentlichen Hand. Zu dieser Gruppe gehören u. a. GeNUA, secunet, Rohde & Schwarz SIT, aber auch T-Systems.
- Ein weitere Sparte, die in Deutschland traditionell der öffentlichen Hand sehr nahe steht, sind **Produkte und Dienstleistungen rund um die elektronische Signatur**. Hierunter fallen z. B.
    - Hardwareanbieter wie KOBIL,

[89] Gartner, 2009

  - Softwareanbieter wie bremen online services oder Applied Security
  - sowie Trust-Center (z. B. D-Trust).

- Eine weitere Nische, in der deutsche Anbieter traditionell stark sind, ist der Bereich **Biometrie** (z. B. DERMALOG).
- Ein Reihe von Anbietern positionieren sich zudem als **Teil größerer Konzerne** und nutzen entsprechende Kapital- , Entwicklungs- und Vertriebsressourcen (z. B. T-Systems, Mühlbauer, Giesecke & Devrient, Rohde & Schwarz SIT, IABG)
- Trotz allem gibt es aber auch in Deutschland mittelständische Anbieter, die mit **standardisierten Produkten** international den Wettbewerb mit den großen Anbietern suchen. Hier sind vor allem Astaro (Firewalls), Avira (Virenschutz), G DATA (Virenschutz) oder auch GSMK (verschlüsselte mobile Sprachkommunikation) zu nennen.

Die unterschiedlichen strategischen Ausrichtungen zeigen sich auch in formellen und informellen Netzwerken, die zwischen den Anbietern existieren, und am Grad der Kooperation mit der Bundesregierung:

- secunet, Mühlbauer und Rohde & Schwarz SIT sind Partner im Rahmen der Sicherheitspartnerschaft mit dem Bundesinnenministerium zur Förderung der nationalen Verschlüsselungstechnik und zur Entwicklung komplexer IT-Sicherheitslösungen im Bereich Hochsicherheit.
- GeNUA, Applied Security, Sirrix, GSMK und andere sind als aktive Mitglieder an der Initiative „IT-Security made in Germany“ (ITSMIG e.V.) des Bundeswirtschaftsministeriums beteiligt und versuchen auf diesem Wege ihre Exportaktivitäten weiter zu entwickeln.
- Bremen online services, Applied Security und secunet fokussieren sich auf die Bereitstellung von spezifischen IT-Sicherheitsprodukten für E-Government-Initiativen der öffentlichen Verwaltung (u. a. elektronische Signatur**).**
- Eine andere Gruppe agiert eher ohne direkte Kooperationen und betreibt eine (erfolgreiche) Internationalisierung ohne größere Mitwirkung staatlicher Stellen, z. B. GSMK, Astaro.

Eine besondere Rolle nimmt das Fraunhofer-Institut für Sichere Informationstechnik (Fraunhofer SIT) ein, das einerseits als Institut der anwendungsorientierten Forschung agiert, andererseits aber auch von den Anbietern als Wettbewerber wahrgenommen wird, nicht zuletzt bei der Vergabe von Geldern der Forschungsförderung oder öffentliche Ausschreibungen.[90]

Kleine Produktanbieter (z. B. GeNUA, Applied Security) kooperieren sehr häufig mit Systemhäusern bzw. großen IT-Dienstleistern (z. B. T-Systems, IBM), um umfassende Lösungen anbieten zu können. Auch zwischen Produktanbietern existieren Vertriebs- bzw. Technologiepartnerschaften. In letzterem Fall werden häufig Kernkomponenten eines Anbieters in Produkte des anderen übernommen: So nutzt z. B. der Anbieter von Firewall Appliances Astaro die Komponente zur Identifizierung von Viren von Avira.

5.3 Deutsche Kernanbieter im Profil

Nachfolgend sollen 18 Unternehmen näher vorgestellt werden, die als repräsentativ für die Gesamtheit der deutschen Anbieter angesehen werden können. Relevant für die Auswahl waren die folgenden Kriterien:

- Unternehmensgröße und technologische Relevanz
- Fokussierung auf IT-Sicherheit
- Ausgewogene Abdeckung der adressierten Marktsegmente
- Repräsentation der typischen Wettbewerbsstrategien (vgl. Abschnitt 5.2.3).

Neben einer allgemeinen Beschreibung des Produktspektrums und des Vertriebsansatzes werden für die einzelnen Anbieter die folgenden Daten strukturiert verglichen:

- **Firmensitz** und **Standorte** in Deutschland
- **Eigentümerstruktur** mit Fokus auf den sich in deutschem Besitz befindlichen Anteilen
- **Aktivität in Deutschland** mit Fokus auf dem Entwicklungs- und Wertschöpfungs- bzw. Dienstleistungsanteil in Deutschland

[90] Interviews mit Anbietern für IT-Sicherheit

- Anzahl der **Mitarbeiter** (für IT-Sicherheit und Deutschland getrennt ausgewiesen)
- **Umsatz** (für IT-Sicherheit und Deutschland getrennt ausgewiesen)
- **Branchenfokus** (insbesondere die Aufteilung zwischen Privatwirtschaft, öffentlicher Hand und Endverbrauchern)
- **Regionaler Fokus** für Aktivitäten außerhalb Deutschlands
- **Angebotsspektrum**, dargestellt anhand der in der Studie durchgängig verwendeten Taxonomie bzw. des Kompetenzrasters
- **Mitgliedschaften** in relevanten Verbänden (z. B. BDI, BITKOM) und Vereinen (z. B. Teletrust e. V., ITSMIG e. V.)

5.3.1 Applied Security GmbH

Übersicht			
Firmensitz/Standorte	Stockstadt am Main		
Eigentümerstruktur	Mehrheitlich im Besitz der deutschen Gründer		
Aktivität Deutschland	Firmenzentrale, Produktentwicklung, Vertrieb		
Mitarbeiter	Ges: 40	IT-S: 40	D: 37
Umsatz (Mio. Euro)	Ges: 2,8	IT-S: 2,8	D: größtenteils
Branchenfokus	Öffentliche Hand, Gesundheit und Finanzdienstleistungen		
Regionaler Fokus	Deutschland (70%) und deutschsprachiger Raum Produktentwicklung ausschließlich in Deutschland		
Angebotsspektrum	• Produktfokus auf: Security Toolkits, Verschlüsselung, Data Loss Prevention, Signatur • Daneben auch: PKI, Beratungsdienstleistungen		
Mitgliedschaften	ITSMIG e. V., BITKOM, Teletrust		

Die Applied Security GmbH ist ein Anbieter von Lösungen und Produkten im Bereich Datensicherheit. Der Schwerpunkt des Produktspektrums liegt in den Bereichen Verschlüsselung, Data Leakage Prevention, digitale Signatur und Authentisierung.

Die fideAS®-Produktfamilie umfasst folgende Module:

- ***fideAS® file enterprise***: unternehmensweit steuerbare Dateiverschlüsselung und Kontrolle mobiler Datenträger
- ***fideAS® sign***: rechtssichere elektronische Signatur
- ***fideAS® health***: sichere Meldungsübertragung an Krankenkassen
- ***fideAS® web***: Verschlüsselung und Signatur von Web-Formularen
- ***fideAS® smile***: Sicherheitstoolkit für Software-Entwickler
- ***fideAS® miniCA***: pragmatische PKI-Lösung.

Im Dienstleistungsbereich bzw. Lösungsgeschäft liegt der Fokus hauptsächlich auf den Sektoren Gesundheit, Finanzdienstleistungen und der öffentlichen Hand. Hauptwettbewerber sind in diesem Umfeld Utimaco, PGP und safeboot. Seit Anfang 2006 besteht ein Joint Venture mit der DRS GmbH, welches den Datenservice für berufsständische Versorgungseinrichtungen zum Gegenstand hat. Der Vertrieb erfolgt im Produktbereich hauptsächlich über Distributoren und Partner im Lösungsgeschäft, vorwiegend direkt.

5.3.2 Astaro AG

Übersicht			
Firmensitz/Standorte	Karlsruhe, Australien, Niederlande, Frankreich, Italien, Japan, Jordanien, Singapur, Schweiz, Großbritannien		
Eigentümerstruktur	Im Besitz der Gründer und der Mitarbeiter sowie eines deutschen und eines amerikanischen Finanzinvestors (mehrheitlich deutsch)		
Aktivität Deutschland	Firmenzentrale, Produktentwicklung, Vertrieb		
Mitarbeiter	Ges: 160	IT-S: 160	D: 100
Umsatz (Mio. Euro)	Ges: ca. 40	IT-S:	D: 45%
Branchenfokus	KMUs und Bildungsbereich (z. B. Schulen in den USA)		
Regionaler Fokus	Exportanteile: Wertschöpfungsanteil in D: Weltweiter Vertrieb mit Schwerpunkten in D, EU, USA		
Angebotsspektrum	• Hauptsegmente: Firewall, Intrusion Detection, Virtual Private Network, Network Access Control, Nachrichten-Sicherheit, Web-Sicherheit • Nebensegmente: Wireless Security, Training Awareness		
Mitgliedschaften	---		

Astaro ist ein Anbieter für Netzwerksicherheit mit Fokus auf kleine und mittelständische Unternehmen und somit auf einfach zu nutzende Produkte. Mit einem „All-in-one"-Ansatz integriert das Unternehmen mehrere Sicherheitslösungen (wie Netzwerkschutz, Webfilter und E-Mail-Sicherheit) in einer einheitlichen Plattform, die auch Managed-Services-Modelle unterstützt. Mit diesem Produkt positioniert sich das Unternehmen als Anbieter von Unified-Threat-Management (UTM). Zu den Hauptprodukten des Unternehmens gehören:

- ***Astaro Security Gateway***: integrierte Netzwerk-, Web- und E-Mail-Sicherheitslösung
- ***Astaro Web Gateway***: Schutz und Kontrolle aller über das Web übertragenen Daten
- ***Astaro Mail Gateway***: Schutz vor Spam-Nachrichten, Viren, Würmern und Trojaner, die durch E-Mails übertragen werden
- ***Astaro Command Center***: zentrale Management-Plattform zur Überwachung und Konfiguration von Astaro-Produkten.

Astaro hat mit 10 internationalen Niederlassungen (USA, Japan, Singapur, Australien sowie mehrere in Europa) und einem Auslandsumsatzanteil von 55% eine internationale Ausrichtung. Alle Produkte werden ausschließlich über Partner vertrieben, sodass sich das Unternehmen auf die Produktentwicklung und Herstellung konzentrieren kann.

5.3.3 Avira GmbH

Übersicht			
Firmensitz/Standorte	Tettnang am Bodensee		
Eigentümerstruktur	In Privatbesitz (deutsch)		
Aktivität Deutschland	Firmenzentrale, Produktentwicklung, Vertrieb		
Mitarbeiter	Ges: ca. 305	IT-S: ca. 305	D: ca. 225
Umsatz (Mio. Euro)	Ges: 17,099	IT-S:	D: ca. 70%
Branchenfokus	Ca. 40% Umsatzanteil mit Privatkunden		
Regionaler Fokus	Deutschland (70%) und deutschsprachiger Raum Produktentwicklung ausschließlich in Deutschland		
Angebotsspektrum	• Produkte zur Erkennung von Schadsoftware (insbesondere Antivirenprogramme) für stationäre und mobile Endgeräte, in Netzwerken und als Komponente in Drittprodukten • Fokus auf Produktentwicklung • Lösungsentwicklung in Zusammenarbeit mit Systemhäusern • Beratung und individueller Support		
Mitgliedschaften	ITSMIG e.V.		

Avira ist ein Anbieter von Anti-Malware-Produkten und insbesondere Antivirusprogrammen. Als Hauptdifferenzierungskriterium gegenüber den Wettbewerbern wird seine Stärke in der proaktiven Erkennung von Schadsoftware gesehen. Diese erfolgt bei Avira anhand typischer Verhaltensmuster der Schadsoftware und nicht nur auf der Basis der Signatur eines Schadprogramms. Durch den Kauf von Datapool im Jahre 2006 wurde eine umfassende Kompetenz im Bereich der Erkennung von Rootkits erworben. Hauptwettbewerber sind neben den großen internationalen Akteuren (z. B. Symantec, McAfee, TrendMicro) vor allem Kaspersky Labs. Als Produktanbieter arbeitet Avira eng mit Systemhäusern, Distributoren und anderen Produktanbietern zusammen (z. B. in dem Sinne, dass ein Avira-Produkt als Antiviruskomponente in Firewallsysteme eingebettet wird). Zu den Hauptprodukten von Avira zählen:

- ***AntiVir:*** Software zum Schutz vor Viren, Würmern, Trojanern und Dialern. In der Basisversion kostenlos und in der Premiumversion inkl. AntiAdware, AntiPhising, MailGuard (POP3 und SMTP), WebGuard für sicheres Surfen
- ***Premium Security Suite:*** Erweiterte Versionen von Antivir-Rundumschutz inkl. z. B. Antispam-, Firewall- und Backup-Funktionen
- ***Business & Enterprise Solutions:*** Produkte, die das gesamte Netzwerk von Firmen einschließlich Desktop-PCs, Dateiservern, Proxyservern, Mailservern und mobilen Endgeräten schützen

5.3.4 bremen online services Gmbh & Co. KG

Übersicht			
Firmensitz/Standorte	Bremen		
Eigentümerstruktur	Stadt Bremen: 55%, Deutsche Telekom: 15%, Sparkasse Bremen: 15%, Brekom GmbH: 12%, BSAG: 3%		
Aktivität Deutschland	Firmenzentrale, Produktentwicklung, Vertrieb		
Mitarbeiter	Ges: 85	IT-S: 85	D: 85
Umsatz (Mio. Euro)	Ges: 6,0	IT-S: 6,0	D: 6,0
Branchenfokus	Starker Fokus auf dem öffentlichen Sektor		
Regionaler Fokus	Hauptsächlich Deutschland		
Angebotsspektrum	• Datensicherheit und Verschlüsselung • Identitäts- und Zugriffsverwaltung, u. a. digitale Signatur • Entwicklung von Sicherheitsstrategien und -architekturen, Trainings		
Mitgliedschaften	BITKOM, Teletrust, Vitako (Arbeitsgemeinschaft der kommunalen Rechenzentren)		

Die bremen online services GmbH & Co. KG entwickelt und vertreibt Software für den rechtsverbindlichen und sicheren Datenaustausch via Internet in Verwaltung, Justiz und Wirtschaft in Deutschland. Die Firma ist Spezialist für elektronische Signaturen und ihren Einsatz zur Rationalisierung von Arbeitsabläufen mit einem Schwerpunkt auf der öffentlichen Verwaltung. Die Firmengründung erfolgte 1999 durch die Stadt Bremen, nachdem diese den Städtewettbewerb MEDIA@Komm, eine Förderinitiative der Bundesregierung (BMWi), gewonnen hatte. Danach war bremen online services u. a. maßgeblich bei der Entwicklung des OSCI-Standards (Online Services Computer Interface) beteiligt, eines Protokollstandards der öffentlichen Verwaltung für die sichere, vertrauliche und rechtsverbindliche Übertragung digitaler Daten.

Die Produkte werden hauptsächlich in Deutschland vertrieben, und zwar sowohl direkt als auch über Partner. Das Unternehmen fokussiert sich auf die Produktentwicklung, bietet daneben aber auch Implementierung und Betrieb sowie Pflege und Weiterentwicklung der Produkte an. Kernprodukt von bremen online services ist die Sicherheitsmiddleware Governikus, eine Anwendung für sichere elektronische Transaktionen im Internet für E-Government, E-Justice und E-Business, die bundesweit und im europäischen Ausland eingesetzt wird.

5.3.5 DERMALOG Identification Systems GmbH

Übersicht			
Firmensitz/Standorte	Hamburg, Kuala Lumpur (Malaysia)		
Eigentümerstruktur	Privatbesitz		
Aktivität Deutschland	Firmenzentrale, Produktentwicklung, Vertrieb		
Mitarbeiter	Ges: N.A.	IT-S:	D:
Umsatz (Mio. Euro)	Ges: N.A.	IT-S:	D:
Branchenfokus	Öffentliche Verwaltung		
Regionaler Fokus	Ausländische Kunden, hauptsächlich in Asien		
Angebotsspektrum	• Fingerabdruck-Identifikationssysteme • Hochsicherheitsdokumente • Chip-, RFID-Karten-, Fingerabdrucklesegeräte		
Mitgliedschaften	BITKOM, ITSMIG e. V., Teletrust		

Dermalog ist ein Anbieter für biometrische Identifikationssysteme. Kernprodukt des Unternehmens ist das „Automatische Fingerabdruck-Identifikations-System“ (AFIS), welches weltweit in national und international operierenden staatlichen Einrichtungen und Firmen verwendet wird. Darüber hinaus bietet das Unternehmen Hochsicherheitsdokumente mit integrierter Biometrie, wie z. B. ID-Cards, Personalausweise, Führerscheine, Gesundheitskarten und andere nationale Identifikationsdokumente oder Zertifikate an. Zu den Hardwareprodukten des Unternehmens zählen Grenzkontrollsysteme, Dokumentenlesegeräte, Chip- und RFID-Kartenlesegeräte, 2D-Barcode-Lesegeräte sowie ein Fingerabdruck-Live-Scanner. Der Vertrieb erfolgt weltweit und wird von der Hamburger Zentrale über strategische Allianzen mit Vertretern, System-Integratoren, lokalen Software-Firmen oder Generalunternehmern gesteuert. Darüber hinaus hat das Unternehmen aufgrund des wachsenden Auftragsvolumens eine Zweigstelle in Kuala Lumpur (Malaysia) für den asiatischen Markt etabliert.

5.3.6 D-TRUST GmbH

Übersicht			
Firmensitz/Standorte	Berlin		
Eigentümerstruktur	100% Tochter der Bundesdruckerei, diese im Bundesbesitz		
Aktivität Deutschland	Firmenzentrale, Produktentwicklung, Vertrieb		
Mitarbeiter	Ges: 51	IT-S: 51	D: 51
Umsatz (Mio. Euro)	Ges: < 10 Mio.	IT-S: 100%	D: 100%
Branchenfokus	50% öffentliche Hand, 50% Privatwirtschaft		
Regionaler Fokus	Ausschließlich in Deutschland tätig		
Angebotsspektrum	PKI-Komponenten (Herausgabe von Signaturkarten, Signaturerzeugung, Validierung und PKI-Verwaltungssoftware)		
Mitgliedschaften	BITKOM, Teletrust, T7		

Die D-Trust GmbH ist ein Trustcenter mit Schwerpunkt auf der qualifizierten elektronischen Signatur und als 100%ige Tochter der Bundesdruckerei im Bundesbesitz. Das Produktspektrum umfasst insbesondere:

- Standard- und Massensignaturkarten, Softtokens und SSL-Zertifikate
- Zeitstempel-Dienste
- Anwender- und Verwaltungssoftware zur digitalen Signatur.

Der Fokus liegt fast ausschließlich auf dem deutschen Markt mit einem 50%-Anteil der öffentlichen Hand. Im Projektgeschäft erfolgt der Vertrieb direkt, im Produktgeschäft auch über Portal- bzw. Anwendungsanbieter.

Wie bei allen Trustcentern ist die weitere Geschäftsentwicklung der D-Trust stark von der massenhaften Verbreitung der qualifizierten Signatur und entsprechender Anwendungen abhängig. Nach Meinung der Anbieter kann diese nur durch entsprechende staatliche Großprojekte (z. B. Jobcard, Gesundheitskarte) erreicht werden. D-Trust ist mit anderen Trustcenter-Betreibern (DATEV eG, Deutsche Post Com GmbH, Deutscher Sparkassenverlag, Deutsche Telekom AG und TC Trustcenter) in der Arbeitsgemeinschaft der Trustcenterbetreiber T7 organisiert, welche als gemeinsame Interessenvertretung agiert.

5.3.7 G Data AG

Übersicht			
Firmensitz/Standorte	Bochum		
Eigentümerstruktur	N/A		
Aktivität Deutschland	Firmenzentrale, Produktentwicklung, Vertrieb		
Mitarbeiter	Ges: 110	IT-S: 110	D: 110
Umsatz (Mio. Euro)	Ges: 22 (2007)	IT-S: 22 (2007)	D: N/A
Branchenfokus	Branchenübergreifend, starker Fokus auf Endverbraucher		
Regionaler Fokus	Schwerpunkt auf Deutschland, aber auch Italien, Frankreich, Benelux-Länder, Spanien, Portugal sowie Japan		
Angebotsspektrum	Antivirenprogramme für stationäre und mobile Endgeräte in Netzwerken, E-Mails, Servern und PCs		
Mitgliedschaften	BITKOM		

Die G Data Software AG ist ein 1985 gegründetes Softwarehaus mit einem Schwerpunkt auf IT-Sicherheitslösungen für Internetsicherheit und Virenschutz. Das Unternehmen führt Produkte für Privatanwender und Unternehmen. Für Privatanwender bietet das Unternehmen eine aufeinander aufbauende Produktpalette an:

- **G Data AntiVirus 2010** zum Schutz gegen Viren, Spyware, Rootkits, Dialer und Phishing-Attacken
- **G Data InternetSecurity 2010** bietet darüber hinaus eine Firewall, Kindersicherung und einen sogenannten „Datenshredder“
- **G Data TotalCare 2010** umfasst als Komplettpaket auch die Datensicherung.

Darüber hinaus werden spezielle Produkte für Notebook- bzw. Netbook-Sicherheit angeboten. Für Unternehmen bietet G Data zusätzlich Produkte mit zentralen Managementfunktionen an. G Data sieht sein Alleinstellungsmerkmal in der Qualitätsführerschaft im Bereich Virenerkennung. Als Argumente hierfür werden die sogenannte Double-Scan-Technologie mit zwei unabhängigen Virenscannern oder der Sofortschutz OutbreakShield aufgeführt.

G Data bewegt sich in einem Segment, welches auch international hart umkämpft ist. Die Vergleichbarkeit der Produkte kommt sich auch in der Vielzahl der Vergleichstests und „Rankings“ einschlägiger Fachzeitschriften zum Ausdruck. Eine gute Platzierung wird hierbei als wichtiger Wettbewerbsfaktor angesehen.

5.3.8 GeNUA

Übersicht			
Firmensitz/Standorte	Kirchheim b. München		
Eigentümerstruktur	100% im Besitz der drei deutschen Unternehmensgründer		
Aktivität Deutschland	Firmenzentrale, Produktentwicklung, Vertrieb		
Mitarbeiter	Ges: 130 (2009)	IT-S: 130 (2009)	D: 130 (2009)
Umsatz (Mio. Euro)	Ges: 10,5	IT-S: 10,5	D: 10,5
Branchenfokus	ca. 50% Privatwirtschaft und 50% öffentliche Hand		
Regionaler Fokus	• Exportanteile über Auslandsniederlassungen deutscher Kunden • Anteil ausländischer Kunden ca. 10% • Schwerpunkt auf dem Persischen Golf		
Angebotsspektrum	• Firewall Appliances (GeNUScreen, GeNUGate) • Datenoptimierung für Satellitenkommunikation • VPN für verschlüsselte Datenübertragung (GeNUCrypt) • System-Management für Netzwerke • Appliance für sicheren mobilen Datenaustausch (GeNUCard) • Awareness-Trainings		
Mitgliedschaften	AFCEA, BayME, BITKOM, Deutsche Gesellschaft für Wehrtechnik e. V., guug, Münchener Kreis, ITSMIG e. V.		

GeNUA (Gesellschaft für Netzwerk- und Unix-Administration) ist ein spezialisierter Anbieter im Bereich Hochsicherheit mit einem Schwerpunkt auf Firewall-Applikationen für die öffentliche Hand, aber auch für andere Branchen wie den Maschinenbau. Die Produkte werden sowohl direkt als auch über verschiedene (kleine und große) Partner vertrieben. GeNUA wurde 1992 gegründet und ist seither kontinuierlich organisch gewachsen. Kernprodukte von GeNUA sind:

- ***GeNUScreen/GeNUGate:*** Firewall-Appliance, zweistufiges Firewallsystem
- ***GeNUCard:*** Appliance für sicheren mobilen Datenaustausch
- ***GeNUBox:*** Sicherheitsplattform für Fernwartung
- ***GenNUCrypt:*** verschlüsselte Datenübertragung innerhalb eines VPN.

Insbesondere der Hochsicherheitsbereich, in dem das Unternehmen u. a. Mitarbeiter mit Sicherheits-Clearance der deutschen Regierung beschäftigt sowie Produkte mit der höchsten Sicherheitszertifizierung anbietet, ist stark auf Deutschland fokussiert. Der internationale Hochsicherheits-Markt im Bereich der öffentlichen Verwaltung ist für das Unternehmen aufgrund von nationalen Sicherheitsbedenken bisher nicht adressierbar. Ausgenommen davon ist der Mittlere Osten, insbesondere die Golf-Staaten. Hauptwettbewerber sind Cisco und Juniper.

5.3.9 Giesecke & Devrient GmbH

Übersicht			
Firmensitz/Standorte	München, 49 Tochtergesellschaften und Joint Ventures in über 30 Ländern		
Eigentümerstruktur	Vollständig in deutschem Familienbesitz		
Aktivität Deutschland	Firmenzentrale, Produktentwicklung, Vertrieb		
Mitarbeiter	Ges: 9849	IT-S: N/A	D: 3800
Umsatz (Mio. Euro)	Ges: 1690	IT-S: ca. 400	D: 251
Branchenfokus			
Regionaler Fokus	Weltweit präsent, Exportanteil: 85%		
Angebotsspektrum	• Integrierte Systeme und Lösungen z. B. für Netzwerk-Authentisierung, E-Mail-Verschlüsselung oder Single Sign-on • Smartcard-basierte Produkte für IT-Sicherheit • Identifikationssysteme für hoheitliche Anwendungen, spezielle Ausweise, Pass- und Visasysteme		
Mitgliedschaften	BITKOM, BVSW, DGFP, DIN, DPRG, EHI, FOGRA, ifo, IHK, IHMA, ITSMIG e. V., TeleTrust Deutschland, VDMA, VDP, Verband Druck und Medien		

Giesecke & Devrient (G&D) ist ein internationaler Anbieter von Banknotenpapier, Banknotendruck, Banknotenbearbeitungssystemen und Karten sowie komplexen Systemlösungen in den Bereichen Telekommunikation, elektronischer Zahlungsverkehr, Gesundheit, Identifizierung und Transport. Zu den IT-Sicherheitsprodukten gehören:

- StarSign: ein übergreifendes System zur Sicherung des geistigen Eigentums (intellectual property) von Unternehmen
- Cards: ID-Kartensyteme, Mobile Security Cards, Reader
- Tokens: Hardwarekomponenten zur Identifizierung und Authentifizierung von Benutzern
- Card Management Systems, die alle Funktionen im Lebenszyklus der Karte steuern

IT-Sicherheit ist mit einem Umsatzanteil von weniger als 10% für G&D nur ein Nebensegment. Mit weltweit 49 Tochtergesellschaften und Joint Ventures in über 30 Ländern ist das Unternehmen stark international ausgerichtet. Die Umsätze stiegen 2008 mit 9% deutlich, bei einem Ergebnis vor Finanzierung und Steuern (EBIT) auf Vorjahresniveau. Das Wachstum soll insbesondere in den internationalen Märkten weiter fortgesetzt werden.

5.3.10 GSMK

Übersicht			
Firmensitz/Standorte	Berlin		
Eigentümerstruktur	Firmenleitung, Mitarbeiter (evtl. auch Investoren)		
Aktivität Deutschland	Firmenzentrale, Produktentwicklung, Vertrieb		
Mitarbeiter	Ges: 25 (2009)	IT-S: (2009)	D: (2009)
Umsatz (Mio. Euro)	Ges: N/A	IT-S: N/A	D: N/A
Branchenfokus	50% öffentliche Hand, 50 % Privatwirtschaft,		
Regionaler Fokus	Umsatz größtenteils außerhalb von Deutschland		
Angebotsspektrum	Encryption von mobiler Kommunikation: Mobiltelefonie, Festnetz, Satelliten, PPX-Gateways		
Mitgliedschaften	ITSMIG e. V.		

Die Gesellschaft für sichere mobile Kommunikation mbH (GSMK) ist ein Anbieter für die Sicherheit von mobiler Sprachkommunikation in den Bereichen Mobiltelefonie, Festnetz, Satelliten und PPX-Gateways. Die Gründung erfolgte im Jahr 2003 durch namhafte Mitglieder des Chaos Computer Clubs (u. a. dessen langjährigen Sprecher Andy Müller-Maguhn). Hauptprodukt von GSMK sind die sogenannten CryptoPhones. Dabei handelt es sich um Mobiltelefone, die eine verschlüsselte Sprachkommunikation in Echtzeit ermöglichen. Als eines der Alleinstellungsmerkmale wird die Veröffentlichung des gesamten Quellcodes angesehen. Dies wird nicht nur aus Gründen der Fehlersuche und Qualitätssicherung als notwendig erachtet, sondern auch um das Vorhandensein von Zugriffsmöglichkeiten Dritter (sog. „Backdoors“) auszuschließen. Dieser Verdacht trifft insbesondere Anbieter von Verschlüsselungsprodukten, die auf nicht öffentlich zugänglichen Protokollen und Technologien basieren. Als weiteres technologisches Alleinstellungsmerkmal wird die gleichzeitige Verwendung zweier Kryptoalgorithmen angesehen, um auch für den Fall, dass eines der Verfahren versagt, die Vertraulichkeit der Sprachübertragung zu gewährleisten. Darüber hinaus werden CryptoPhones auch als Festnetztelefon und als Softwaretelefon für Windows angeboten.

5.3.11 IABG mbH

Übersicht			
Firmensitz/ Standorte	Ottobrunn, weitere 11 Standorte in Deutschland und in der EU		
Eigentümerstruktur	im Besitz der deutschen Unternehmensführung		
Aktivität Deutschland	Firmenzentrale, Produktentwicklung, Vertrieb		
Mitarbeiter	Ges: 1027	IT-S: 135	D: 135
Umsatz (Mio. Euro)	Ges: 140	IT-S: 22	D: 22
Branchenfokus	- Öffentl. Verwaltung (40%), - Verkehr und Logistik, Automotive, Energieversorger (60%)		
Regionaler Fokus	D, EU Institutionen		
Angebotsspektrum	▪ Entwicklung von IT-Sicherheitsstrategien/Durchführung von IT-Sicherheitsanalysen und -zertifizierungen ▪ Identitätsmanagement, PKI ▪ Digitale Signaturen ▪ Managed Security Services ▪ Sichere Kommunikationsnetze		
Mitgliedschaften	BDLI, BITKOM, DWT, FKH, ZVEI, TeleTrust		

Die IABG wurde 1961 auf Initiative des Bundes als zentrale Analyse- und Testeinrichtung für die Luftfahrtindustrie und das Verteidigungsministerium gegründet und ist heute ein technisch-wissenschaftliches Dienstleistungsunternehmen. Das Dienstleistungsspektrum der IABG umfasst analytische, technische und operationelle Lösungen in den Branchen: Automotive, Info-Kom, Verkehr & Umwelt, Luftfahrt, Raumfahrt und Verteidigung & Sicherheit. Das Unternehmen wurde 1991 privatisiert und wird heute von ihren Eigentümern geführt.

Im Bereich IT-Sicherheit unterhält das Unternehmen zwei Geschäftsbereiche. Der Geschäftsbereich IT-SEC Beratung umfasst die Entwicklung von Sicherheitsstrategien sowie die Durchführung von Sicherheitsanalysen. Der Geschäftsbereich INFO-KOM bietet schwerpunktmäßig sichere Kommunikationsnetze wie Digitalfunk (BOS) mobile ad-hoc Netze (HiMoNN) und Satelliten Kommunikation (Teleport) an. Darüberhinaus gehören Managed Security Services (u.a. Management von Firewalls oder VPN) sowie Lösungen für Identitätsmanagement und -verwaltung, Public Key Infrastrukturen sowie für die digitale Signatur (AQSigMail) zum Angebotsspektrum der IABG.

Die IABG vertreibt ihre Produkte ausschliesslich direkt und überwiegend in Deutschland sowie mit wachsendem Erfolg bei den europäischen Institutionen in Brüssel.

5.3.12 KOBIL

Übersicht			
Firmensitz/Standorte	Worms, Istanbul		
Eigentümerstruktur	Alleiniger geschäftsführender Gesellschafter: Ismet Koyun		
Aktivität Deutschland	Firmenzentrale, Produktentwicklung, Vertrieb		
Mitarbeiter	Ges: 50 (2007)	IT-S: 50 (2007)	D: N/A
Umsatz (Mio. Euro)	Ges: 15 (2008)	IT-S: 15 (2008)	D: N/A
Branchenfokus	Finanzdienstleister, insb. Banken		
Regionaler Fokus	Europa, hohe Marktanteile in Deutschland und der Türkei		
Angebotsspektrum	• Identitätsmanagement • Kryptographie • Smartcard-Technologie • PKI (digitale Zertifikate)		
Mitgliedschaften	Teletrust		

KOBIL agiert als Hersteller hochsicherer Basistechnologie im Umfeld von Smartcards, Einmalpasswörtern (OTP) und Zertifikaten. Das Produktangebot basiert auf eigenen Forschungs- und Entwicklungsarbeiten. Im besonderen Fokus stehen die Online-Anwendungen der Banken im nationalen und internationalen Geschäftsverkehr für Geschäfts- und Privatkunden. Wichtige Referenzkunden im Bankenumfeld sind die Commerzbank, die Sparkassen, die Volks- und Raiffeisenbanken, ferner Telekommunikationsunternehmen (z. B. Deutsche Telekom, Swisscom, Arcor/Vodafone).

Das Kerngeschäft des Unternehmens liegt traditionell in der Entwicklung und Herstellung von Lesegeräten für Smartcards. Mittlerweile bietet das Unternehmen drei Produktlinien an:

- Smartcards bzw. Smarttokens zur sicheren Identifikation (mIDentity), die u. a. in Kooperation mit der Firma Applied Security in Verbindung mit deren Online-Banking-Applikation angeboten werden
- One-time-Password-Systeme: Geräte, die im Rahmen einer Zwei-Faktoren-Authentifikation ein Zufallspasswort generieren, das zusammen mit einer PIN den Zugang zu einem System ermöglicht
- Smartcard-Terminals (TriBank/TriCAP)

Alle Produkte werden sowohl direkt als auch über ein Partnernetzwerk vertrieben.

5.3.13 Mühlbauer

Übersicht			
Firmensitz/Standorte	Roding		
Eigentümerstruktur	börsennotiert		
Aktivität Deutschland	Firmenzentrale, Produktentwicklung, Vertrieb		
Mitarbeiter	Ges: 1900	IT-S:	D:
Umsatz (Mio. Euro)	Ges: 173	IT-S:	D:
Branchenfokus			
Regionaler Fokus	Technologiezentren in Deutschland, Malaysia, den USA und der Slowakei		
Angebotsspektrum			
Mitgliedschaften	Sicherheitspartnerschaft des BMI		

Mühlbauer ist ein Anbieter für System- und Softwarelösungen zur Produktion und Personalisierung von Karten, Reisepässen und RFID-Anwendungen.

Die Aktivitäten des Unternehmens gliedern sich in folgende Segmente:

Cards & TECURITY: Softwarelösungen und Produkte zur Erfassung von Daten; Produktion und Personalisierung von Karten und Reisepässen; kontaktlose Karten, Aufkleber, Tickets oder Kofferbänder; individuelle Lösungen für die industrielle Bildverarbeitung von Karten, Münzen, Banknoten, Tuben

Semiconductor Related Products und Traceability: Anlagen für flexible Solarzellen und Verpackungsgurte für spezifische Nischenanwendungen im Halbleiterbereich (Semiconductor Related Products)

Precision Parts & Systems: Präzisionsteile zur Fertigung der eigenen Produkte und für sensible Industrien wie z. B. die Luft- und Raumfahrt, den Motorsport oder die Medizin- oder Halbleiterindustrie.

5.3.14 Rohde & Schwarz SIT GmbH

Übersicht			
Firmensitz/Standorte	München, Standorte in 70 Ländern		
Eigentümerstruktur			
Aktivität Deutschland	Firmenzentrale, Produktentwicklung, Vertrieb		
Mitarbeiter	Ges: 150	IT-S:	D: 150
Umsatz (Mio. Euro)	Ges: ca. 30	IT-S:	D: ca. 20
Branchenfokus	80% öffentliche Verwaltung		
Regionaler Fokus	Weltweiter Vertrieb über die Muttergesellschaft, Fokus auf Deutschland		
Angebotsspektrum	• Fokus auf Software- und Hardware-Lösungen (Komponenten) für die sichere mobile Kommunikation (GSM, ISDN) • Verschlüsselungslösungen für analoge, digitale, kabel- und funkbasierte, vermittelte und festgeschaltete Verbindungen • Analyse-, Beratungs- und Integrationsleistungen zur Informations- und Kommunikationssicherheit • Kundenspezifische Software- und Hardware-Lösungen		
Mitgliedschaften	BITKOM, Teletrust, Sicherheitspartnerschaft mit BMI		

Die Rohde & Schwarz SIT GmbH bietet vom Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie von NATO und SECAN zugelassene Lösungen für die Sicherheit in der Informations- und Kommunikationstechnik. Im Mittelpunkt steht die Entwicklung von Kryptoprodukten und -systemen zum Schutz von Informationen in modernen Datenverarbeitungs- und Kommunikationssystemen sowie die Beratung von und IT-Sicherheitsanalysen für Politik, Behörden, Streitkräfte und Wirtschaft. Das Unternehmen ist ein 100%iges Tochterunternehmen von Rohde & Schwarz und liefert seine Verschlüsselungskomponenten auch an den Mutterkonzern. Das Unternehmen vertreibt alle Produkte direkt schwerpunktmäßig an Kunden in Deutschland. Seit 2004 besteht eine Sicherheitspartnerschaft mit dem BMI zur Förderung nationaler Verschlüsselungstechnik und zur Entwicklung komplexer IT-Sicherheitslösungen im Bereich Hochsicherheit.

5.3.15 secunet Security Networks AG

Übersicht			
Firmensitz/Standorte	Essen, acht weitere Standorte in Deutschland, jeweils ein Standort in der Schweiz und in der Tschechischen Republik		
Eigentümerstruktur	76% Giesecke & Devrient, 24% Streubesitz		
Aktivität Deutschland	Firmenzentrale, Produktentwicklung, Vertrieb		
Mitarbeiter	Ges: 265	IT-S:	D:
Umsatz (Mio. Euro)	Ges: 52 (2008)	IT-S:	D: >40 (2008)
Branchenfokus	80% der Umsätze im öffentlichen Sektor, Automobil, Luftfahrt		
Regionaler Fokus	Exportanteile: Auslandsumsatz in 2008: 11,4 Mio. Euro		
Angebotsspektrum	• Netzsicherheit & Verschlüsselung • PKI und Identitätsmanagement • Signaturen • Biometriesysteme und -komponenten • Systemintegration und Consulting Services • Schulungen		
Mitgliedschaften	ITSMIG e.V., TeleTrust, BitKom, Sicherheitspartnerschaft mit BMI		

secunet ist ein Spezialist für IT-Sicherheit mit Schwerpunkt auf den Themen Kryptographie, E-Government, Business Security und Automotive Security. Dabei liegt der Fokus auf der Kombination der Sicherung von IT-Infrastrukturen mit Prozessoptimierung.

Der Vertrieb erfolgt sowohl direkt als auch über Partner hauptsächlich in Deutschland, aber auch international (Niederlande, Schweiz, Baltikum, Skandinavien und Ägypten). Zudem gehören internationale Institutionen bzw. Organisationen, wie die EU-Kommission, Eurocontrol oder die NATO zu den Kunden des Unternehmens. Die Internationalisierung des Geschäfts zählt zu den Schwerpunkten für dieses und die kommenden Jahre. Eines der wichtigsten Produkte für den öffentlichen Sektor ist die sog. Sinabox, welche geschützte oder behördlich klassifizierte Netze als VPN-Gateway über das Internet verbindet.

Seit 2004 konnte secunet ein durchschnittliches Umsatzwachstum von 13% erzielen. Nach einer deutlichen Steigerung von 26% im Jahre 2008 wird aufgrund der guten Auftragslage auch für 2009 ein anhaltendes Umsatzwachstum erwartet. Das Unternehmen profitiert dabei u. a. vom Konjunkturprogramm der Bundesregierung.

5.3.16 Sirrix AG security technologies

Übersicht			
Firmensitz/Standorte	Saarbrücken, Bochum		
Eigentümerstruktur	100% deutscher Familienbesitz		
Aktivität Deutschland	Firmenzentrale, Produktentwicklung, Vertrieb		
Mitarbeiter	Ges: 60	IT-S:	D:
Umsatz (Mio. Euro)	Ges: 1,8 (2008)	IT-S: 90%	D:
Branchenfokus	80% Regierungsgeschäft		
Regionaler Fokus	50% des Umsatzes werden außerhalb von Deutschland erzielt		
Angebotsspektrum	• Sicherheit von Kommunikationsinfrastrukturen und Betriebssystemen • Sicherheit von Netzwerken • Datensicherheit (Encryption)		
Mitgliedschaften	ITSMIG e. V., TeleTrust, Trusted Computing Group, eurobits		

Die Sirrix AG ist ein Spin-Off-Unternehmen der Universität des Saarlandes und wurde von Mitarbeitern der Arbeitsgruppen für Kryptographie, Sicherheit, Deduktions- und Multiagentensysteme gegründet. Das Angebotsspektrum beinhaltet Sicherheitsberatung, die Konzeption und Entwicklung von Sicherheitslösungen für Telekommunikationsinfrastrukturen und -systeme sowie den Entwurf, die Analyse und die Entwicklung kryptographischer Protokolle und Verfahren. 80% des Geschäfts wird mit Regierungsorganisationen (BSI, Pentagon, NATO) erzielt. Die Firma vermarktet alle Produkte an Unternehmen und Behörden im In- und Ausland im Direktvertrieb. Der Direktvertrieb der Produkte erfolgt über Online-Vertriebsplattformen. Zu den Sirrix-Produkten gehören u. a.:

- ***Sirrix.TrustedVPN Appliances:*** Geräte zur Sicherung von VPN-Netzwerken
- ***Sirrix.Security Gateways:*** abhörsichere Mobilkommunikation
- ***Turaya:*** Security-Framework, das auf der Isolation sicherheitskritischer Anwendungen basiert und zur Durchsetzung von Sicherheits-Policies dient

Aufgrund der guten Geschäftsentwicklung erwartet Sirrix für 2009 eine deutliche Umsatzsteigerung.

5.3.17 T-Systems – Enterprise Services GmbH

Übersicht			
Firmensitz/Standorte	Frankfurt am Main		
Eigentümerstruktur	100% Tochter der Deutschen Telekom		
Aktivität Deutschland	Firmenzentrale, Produktentwicklung, Vertrieb		
Mitarbeiter	Ges: 46.000	IT-S: 1000	D: >900
Umsatz (Mio. Euro)	Ges: 9300	IT-S: 500–2000	D: 90%
Branchenfokus	Öffentliche Hand		
Regionaler Fokus	Exportanteile: Wertschöpfungsanteil in D: ?		
Angebotsspektrum	• Identity and Access Management • Enterprise Security Management • Seamless ICT Infrastructure Security		
Mitgliedschaften	BITKOM, Teletrust		

T-Systems ist ein internationaler Betreiber von Informations- und Kommunikationstechnik für multinationale Konzerne und öffentliche Institutionen. Das Unternehmen ist eine Tochter der Deutschen Telekom AG und positioniert sich als „Konvergenz"-Lösungsanbieter, der Informationstechnik und Telekommunikation integriert. Seit 2008 konzentriert sich T-Systems auf das Großkundengeschäft mit 400 multinationalen Unternehmen sowie Kunden aus dem öffentlichen und dem Gesundheitssektor.

Im Bereich IT-Sicherheit bietet das Unternehmen u. a. Identitäts- und Zugriffsverwaltung, Verwaltung der Unternehmenssicherheit und „Seamless ICT Infrastructure Security", und zwar sowohl in Form standardisierter Services und Lösungen als auch auf den einzelnen Kunden zugeschnittener Lösungen. Darüber hinaus gehören alle produktspezifischen Dienstleistungen zum Produktspektrum des Unternehmens, die die Konzeption, die Implementierung, den Betrieb und die Verwaltung im Rahmen eines „Seamless ICT Infrastructure Security"-Ansatzes betreffen, sowie Sicherheitsüberprüfungen und Sicherheitsstrategien und -architekturen. T-Systems agiert in der IT-Sicherheit jedoch nicht als Produktanbieter, sondern kooperiert mit (oft kleineren) Unternehmen, um gesamthafte Lösungen anbieten zu können.

5.3.18 TÜV Informationstechnik GmbH

Übersicht			
Firmensitz/Standorte	Essen, Siegen, Augsburg		
Eigentümerstruktur	100% im Besitz der TÜV NORD Gruppe		
Aktivität Deutschland	Firmenzentrale, Produktentwicklung, Vertrieb		
Mitarbeiter	Ges: 80	IT-S: 50	D: 80
Umsatz (Mio. Euro)	Ges:	IT-S:	D:
Branchenfokus	Breite Abdeckung der Industrien, aber Fokus auf IT (Zertifizierung von Herstellern)		
Regionaler Fokus	Export hauptsächlich EU, Asien, USA		
Angebotsspektrum	▪ Prüfung von Qualität, Funktionalität und Sicherheit von IT-Produkten ▪ Sicherheitsevaluationen und -validierungen ▪ Netzwerksicherheitsanalysen ▪ Informationssicherheits-Management (ISMS) ▪ Konformitätsprüfungen ▪ IT-Security-Trainings und IT-Consulting ▪ Unterstützung ausländischer Behörden beim Aufbau eigener Prüfstellen (z. B. Japan, Korea, Taiwan, Indien)		
Mitgliedschaften	BITKOM, Teletrust, ITSMIG e. V.		

Die TÜV Informationstechnik GmbH (TÜViT) ist Bestandteil der TÜV Nord Gruppe und innerhalb dieses Konzerns auf die Bewertung, Prüfung und Zertifizierung (insbesondere technische Zertifizierung) von IT-Produkten, IT-Systemen und IT-Prozessen spezialisiert. Dabei geht es zum einen darum, zu überprüfen, ob Gesetze, Richtlinien und vertragliche Anforderungen eingehalten werden, aber auch darum, die Vertrauenswürdigkeit von IT-Sicherheitskomponenten zu verbessern, was für den Vertrieb von IT-Sicherheitsprodukten eine große Rolle spielt (vgl. Abschnitt **4.7.4**) Das Unternehmen ist im In- und Ausland tätig und konnte in der Vergangenheit eine kontinuierliche Umsatzsteigerung erzielen.

Im Bereich der IT-Sicherheit bietet TÜViT u. a. Sicherheitsprüfungen nach europäischen und internationalen Standards sowie spezifischen Sicherheitskriterien an. Im Bereich des Datenschutzes bietet TÜViT Prüfungen von IT-Produkten und Dienstleistungen nach deutschen und europäischen Datenschutzbestimmungen an. Auch innerhalb der TÜV Süd Gruppe existiert mit der TÜV SÜD Informatik und Consulting Services GmbH eine auf IT-Sicherheit spezialisierte Einheit.

5.4 Globale Anbieter mit relevanter deutscher Marktposition

Im deutschen IT-Sicherheitsmarkt sind eine Vielzahl internationaler Anbieter mit zum Teil signifikanter Marktposition vertreten. Größter internationaler Anbieter für IT-Sicherheitsprodukte ist mit einem weltweiten Marktanteil von 13% die US-amerikanische Firma Symantec, gefolgt von Cisco mit 9% und McAfee mit 7% Marktanteil.[91]

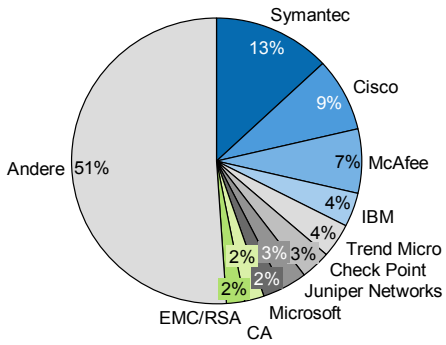


Abbildung 30: IT-Sicherheitsprodukte – Marktanteile weltweit

Auf dem deutschen Markt dominieren die internationalen Anbieter insbesondere das Segment der IT-Sicherheitssoftware, wo sich, aufgrund der einfachen Skalierbarkeit der Softwareprodukte, Kostenvorteile für große Anbieter gegenüber lokalen Spezialanbietern ergeben. In diesem Segment hat in Deutschland daher kein inländischer Anbieter signifikante Marktanteile. Führend ist Symantec mit einem Marktanteil von 23%, gefolgt von McAfee mit 9%.[92]

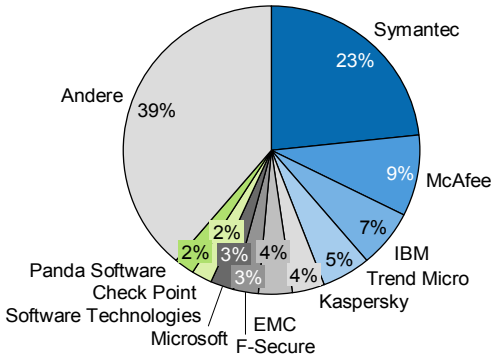


Abbildung 31: IT-Sicherheitssoftware – Marktanteile Deutschland

Im Folgenden werden die wichtigsten internationalen Anbieter für IT-Sicherheitsprodukte im Profil dargestellt.

---

[91] IDC, 2009

[92] Gartner, 2009

5.4.1 Symantec

Firmensitz	Cupertino, USA; in Deutschland: Aschheim
Mitarbeiter	17.400, davon in Deutschland: 400
Umsatz (Mio. USD)	6.149, davon IT-Sicherheit: 2914,1

Das börsennotierte US-Unternehmen Symantec ist der weltweit führende Anbieter für IT-Sicherheit. Das Angebot des Unternehmens konzentriert sich auf Sicherheits-, Speicher- und Systemverwaltungslösungen, die Unternehmen und Privatpersonen bei der Absicherung und Verwaltung ihrer Daten unterstützen. Insbesondere im Bereich IT-Sicherheitssoftware ist das Unternehmen Marktführer. Wie in Abschnitt 5.2.2 beschrieben, ist Symantec in der Vergangenheit durch Unternehmenszukäufe signifikant gewachsen und hat sein Angebotsspektrum dabei deutlich erweitert. Symantec vertreibt seine Produkte über ein weitreichendes Partnernetzwerk in über 40 Länder, bietet einige Produkte aber auch im Direktvertrieb online an. Als Stärken des Unternehmens gelten die schnelle Integration erworbener Unternehmen sowie erfolgreiche Technologiepartnerschaften, u. a. mit Juniper und Accenture.

5.4.2 Cisco

Firmensitz	San José, USA; in Deutschland: Hallbergmoos bei München, Berlin, Bonn, Hamburg, Düsseldorf, Eschborn und Stuttgart
Mitarbeiter	66.000, davon in Deutschland: 850
Umsatz (Mio. USD)	39.500, davon IT-Sicherheit: 1909,6

Das im Jahre 1984 gegründete US-Unternehmen Cisco Systems, Inc. entwickelt und produziert Internet-Protokoll-basierte (IP-basierte) Netzwerklösungen sowie damit im Zusammenhang stehende Produkte der Kommunikations- und Informationstechnologie. Bekannt ist Cisco vor allem für seine Router und Switches, die einen großen Teil des Internet-Backbones versorgen. Die Produkte werden auch in Verbindung mit umfangreichen Dienstleistungen angeboten. Zum Angebotsspektrum des IT-Sicherheitsbereichs gehören Firewalls, Virtual Private Networks, Intrusion Prevention sowie E-Mail- und Web-Sicherheit.

Die Niederlassungen in Deutschland haben vor allem eine Vertriebs- und Marketingfunktion, unterstützen aber auch den technischen Support und das Channel-Management. Die Branchenschwerpunkte des Unternehmens liegen auf dem öffentlichen Sektor und der Telekommunikationsbranche.

5.4.3 McAfee

Firmensitz	Santa Clara, USA; in Deutschland: München, Hamburg
Mitarbeiter	5500, davon in Deutschland: nicht bekannt
Umsatz (Mio. USD)	1614, davon IT-Sicherheit: 1.614

Das US-Unternehmen McAfee ist ein weltweit agierender Spezialist für IT-Sicherheitssoftware. Das Unternehmen wurde 1987 gegründet und ist heute börsennotiert. Das Angebotsspektrum reicht von Antivirusprodukten für Privatcomputer über integrierte Lösungen für Desktops, Server und Netzwerke kleinerer und mittelgroßer Unternehmen (auch als SaaS-Konzept) bis hin zum Schutz der kompletten IT-Infrastruktur von Großunternehmen und Organisationen inkl. aller mobilen Endgeräte. Das Unternehmen ist durch zahlreiche Akquisitionen (u. a. Solidcore im Juni 2009) stark gewachsen und konnte die Umsätze in den letzten drei Jahren um durchschnittlich 18% steigern. Der Umsatz wird zu rund 40% mit Privathaushalten und zu 60% mit Unternehmen und Organisationen erzielt. Als Stärken gelten die gute Performance hinsichtlich Umsatz und Ergebnisentwicklung sowie die strategische Partnerschaft mit weltweit 55 Unternehmen in einer Security Innovation Alliance.

5.4.4 Trend Micro

Firmensitz	Tokio, Japan; in Deutschland: Halbergmoos
Mitarbeiter	3600, davon in Deutschland: nicht bekannt
Umsatz (Mio. USD)	848, davon IT-Sicherheit:834,4

Trend Micro ist ein börsennotierter Anbieter von Software und Dienstleistungen in den Bereichen Virenschutz für Netzwerke und Internet Content Security. Seit seiner Gründung im Jahr 1988 bietet das Unternehmen Privatpersonen und Unternehmen jeder Größe Sicherheitslösungen zum Schutz vor einer Vielzahl von Bedrohungen wie z. B. Viren, Spam, Phishing, Spyware, Bot-Netzen und anderen Internet-Bedrohungen (z. B. Datendiebstahl durch Malware) an. Der Bekanntheitsgrad des Unternehmens wurde 2004 durch die Entscheidung von Hotmail, Mails und E-Mail-Anhänge mit Trend-Micro-Software nach Viren zu durchsuchen, deutlich gesteigert. Trend Micro vertreibt seine Produkte weltweit in mehr als 50 Ländern durch Corporate- und Value-Added-Reseller sowie Dienstleister und auch direkt über die eigene Website.

5.4.5 Check Point Software Technologies Ltd.

Firmensitz/Standorte	Redwoon City, USA; in Deutschland: Ismaning
Mitarbeiter	ca. 1880, davon in Deutschland: 40
Umsatz (Mio. USD)	808, davon IT-Sicherheit: 774,2

Das 1993 in Israel gegründete Unternehmen Check Point Software Technologies Ltd. entwickelt, vermarktet und leisten den Support für eine Vielzahl von Softwareprodukten und kombinierten Hardware- und Softwarekomponenten für IT-Sicherheit. Zum Produktportfolio gehören ferner Netzwerk- und Gateway-Security-Lösungen sowie Daten- und Endgerätesicherheitsprodukte. Die Lösungen arbeiten unter einer einheitlichen Sicherheitsarchitektur, die eine zentrale Steuerung der Endgerätesicherheit sowie die Integration von Produkten anderer Anbieter ermöglicht. Nach dessen eigenen Angaben nutzen sämtliche Fortune-Top-100-Unternehmen Sicherheitslösungen des Unternehmens. In 2008 hat Check Point den Bereich Sicherheitstechnik von Nokia übernommen und erweitert damit sein bisheriges Produktportfolio um weitere Hardwarelösungen.

5.4.6 Juniper Networks

Firmensitz	Sunnyvale, USA; in Deutschland: Vertriebsniederlassungen in Frankfurt und München
Mitarbeiter	7000, davon in Deutschland: ca. 90
Umsatz (Mio. USD)	3570, davon IT-Sicherheit: 580,5

Juniper Networks ist der weltweit zweitgrößte IT-Netzwerkausrüster. Das Unternehmen wurde im Jahre 1996 gegründet und ist seit 1999 börsennotiert. Im IT-Sicherheitsmarkt bietet Juniper Produkte im Bereich Intrusion Detection & Prevention und Netzwerksicherheit (Firewall und VPN) für die Privatwirtschaft und Behörden an. In der Zeit von 1999 bis 2005 ist das Unternehmen vor allem durch eine Reihe von Übernahmen schnell gewachsen. In den letzten Jahren erreichte Juniper aber auch ein starkes organisches Wachstum (26% in 2008). Juniper betreibt Vertriebsniederlassungen in mehr als 40 Ländern weltweit und vertreibt seine Produkte zudem über ein umfangreiches Netzwerk von Partnern und Distributoren.

5.4.7 CA

Firmensitz	Islandia (NY), USA; in Deutschland: Darmstadt
Mitarbeiter	13.700, davon in Deutschland: nicht bekannt
Umsatz (Mio. USD)	4271, davon IT-Sicherheit: 462,7

CA ist weltweit einer der größten Anbieter von IT-Management-Software. Das Unternehmen mit Hauptsitz in den USA wurde 1976 gegründet und betreibt heute weltweit 150 Niederlassungen in mehr als 45 Ländern. Nach eigenen Angaben zählt CA nahezu alle Fortune-1000-Unternehmen zu seinen Kunden. Im IT-Sicherheitsbereich werden hauptsächlich folgende Produkte vertrieben: Data & Resource Protection (Kontrolle des Zugriffs auf Informationen), Secure Web Business Enablement (zentrale Sicherung des Zugangs zu Webanwendungen) und Security Information Management (Erfassung und Archivierung von Protokolldaten für Compliance-Reporting). Die Wachstumsstrategie des Unternehmens stützt sich auf die vier Pfeiler Produktentwicklung, partnerschaftliche Zusammenarbeit, globale Expansion sowie strategische Übernahmen.

5.4.8 EMC

Firmensitz	Hopkinton, USA; in Deutschland: Schwalbach
Mitarbeiter	42.000, davon in Deutschland: 1000
Umsatz (Mio. USD)	14.880, davon IT-Sicherheit: 419,7

EMC ist ein Anbieter von Technologien und Lösungen für Informationsinfrastrukturen. Zu den Produkten im IT-Sicherheitsbereich gehören die Sicherung und Verfolgung sensibler Informationen innerhalb und außerhalb der Firewall oder die Verschlüsselung von Dateispeichern, Zugriffskontrollen und elektronischen Signaturen (Documentum Trusted Content Services). Mit dem „Smarts Application Discovery Manager“ bietet EMS eine Software zum Auffinden und Aufzeichnen aller Anwendungen, die Zugriff auf sensible Informationen haben, an. Die unternehmenseigene Tochter RSA, welche im Jahre 2007 für 2 Mrd. USD übernommen wurde, vertreibt Produkte in den Bereichen Authentifikation, Identitäts- und Zugangskontrolle, Data Loss Prevention, Encryption, Compliance and Security Information Management sowie Fraud Prevention.

Fazit

Der Vergleich der deutschen Anbieter für IT-Sicherheit mit den weltweit führenden Unternehmen dieser Branche ist, wie die folgende Abbildung zeigt, ein Vergleich David gegen Goliath. Mit Ausnahme der T-Systems und Giesecke & Devrient existieren in Deutschland keine global operierenden Anbieter, die einen Umsatz von mehr als 100 Mio. Euro haben.

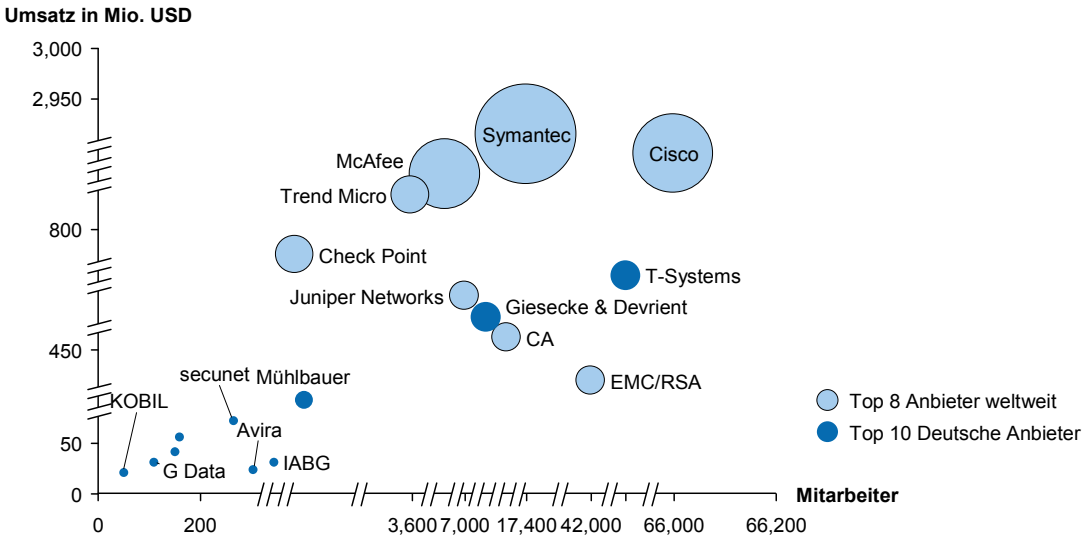


Abbildung 32: Vergleich deutscher Anbieter mit weltweit führenden Unternehmen nach Umsatz (2007) und Anzahl Mitarbeiter[93]

[93] IDC 2009, Booz & Company Analyse

6 Stärken- und Schwächenprofil

6.1 Die Positionierung deutscher Anbieter in den einzelnen Marktsegmenten

Auf der Basis der in Abschnitt 5.1 beschriebenen Struktur der deutschen Anbieterlandschaft und der Einzelprofile der ausgewählten Anbieter wird im Folgenden die Positionierung deutscher IT-Sicherheitsfirmen innerhalb der einzelnen Marktsegmente analysiert. Diese Marktabdeckung wird außerdem mit der zuvor entwickelten Taxonomie abgeglichen, um Stärken und Lücken zu identifizieren. Dieser Abgleich kann naturgemäß nicht *sämtliche* deutschen IT-Sicherheitsanbieter umfassen. Die Auswahl der eingehender analysierten Unternehmen innerhalb der deutschen IT-Sicherheitsbranche ist jedoch keineswegs willkürlich, sondern umfasst die exponierten Unternehmen, die sich durch eine signifikante Größe auszeichnen. Die berücksichtigten Unternehmen wurden also aufgrund ihrer Stellung im bzw. wegen ihrer Aussagekraft für den Markt ausgewählt.

Zusammenfassend lässt sich auf der Produktseite generell ein Schwerpunkt im Segment **Identitäts- und Zugriffsverwaltung** erkennen. Hier sind die deutschen Unternehmen auch in allen Untersegmenten wie User/Authorization Management, Strong Authentication, Smartcards und PKI signifikant vertreten. Auch Experton sieht die deutschen Anbieter in diesem Bereich besonders gut aufgestellt.[94] Unternehmen, die Produkte im Segment Identitäts- und Zugriffsverwaltung anbieten, sind u. a. D-Trust, bremen online services, Giesecke & Devrient und Dermalog. Darüber hinaus sind die deutschen Anbieter im Segment **Netzwerksicherheit** und hier insbesondere in den Untersegmenten Firewalls, Intrusion Detection & Prevention sowie Virtual Private Networks positioniert. Firewalls, die zum Teil auch Hochsicherheitsstandards erfüllen, werden beispielsweise von GeNUA angeboten. Im Bereich der Endgerätesicherheit bieten deutsche Unternehmen Produkte in den Untersegmenten Personal Firewall und Anti-Malware an.

Im Segment **Datensicherheit** sind die deutschen Unternehmen lediglich im Bereich der Verschlüsselung („Encryption") stärker vertreten (u. a. Applied Security, secunet, Giesecke & Devrient). In den anderen Bereichen der Daten-

[94] Interview mit Experton Analyst, 2009

sicherheit wie Data Loss Prevention und Digital Rights Management sind die deutschen Anbieter schlechter positioniert. Dies ist auch für die Segmente Applikationssicherheit sowie serverseitige Web- und E-Mail-Sicherheit der Fall.

Was den Lebenszyklus der Produkte (vgl. 3.4) betrifft, liegt der Fokus v. a. auf der Entwicklung und Herstellung. Insbesondere im Segment Identitätsmanagement spielen aber auch die Konzeption und das Management bzw. der Betrieb der Systeme eine wichtige Rolle.

In der folgenden Abbildung ist die derzeitige Abdeckung der IT-Sicherheitstaxonomie durch deutsche IT-Sicherheitsanbieter nach Segmenten und Untersegmenten sowie Stufen im Lebenszyklus dargestellt.

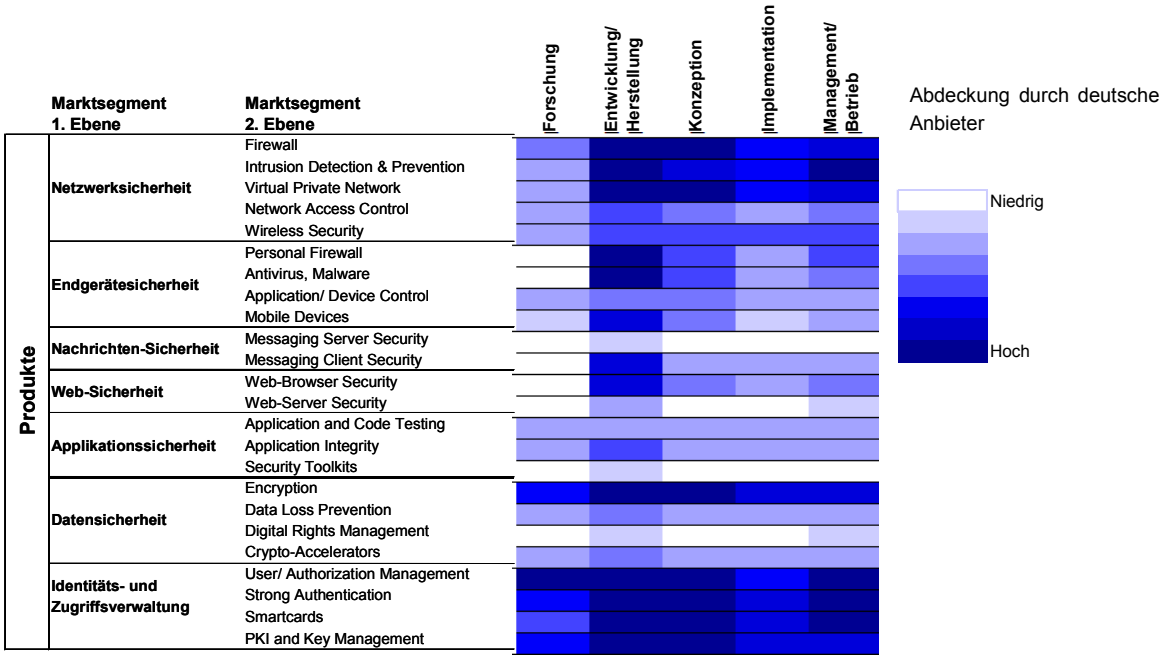


Abbildung 33: Produkt-Angebotsstruktur der IT-Sicherheitsfirmen im deutschen Markt[95]

Die IT-Sicherheitsdienstleistungen lassen sich einteilen in produktbezogene Dienstleistungen (Lösungskonzeption, Implementierung, Betrieb oder gar Management der Systeme), die in ähnlicher Weise auch für andere IT-Anwendungen und IT-Systeme erbracht werden, einerseits und spezielle IT-

[95] Booz & Company Analyse

Sicherheitsdienstleistungen andererseits. Der Bereich der produktbezogenen Dienstleistungen wird nur zum Teil auch von den Produktanbietern abgedeckt, sondern häufig den etablierten IT-Dienstleistungsunternehmen überlassen. Die Situation der deutschen Anbieter ähnelt hierbei derjenigen im gesamten IT-Markt: Deutsche IT-Dienstleister wie z. B. T-Systems spielen im nationalen Umfeld durchaus eine bedeutende Rolle. Ein Großteil des deutschen Marktes und viel mehr noch der globale Markt wird jedoch von internationalen IT-Dienstleistern, insbesondere aus den USA (z. B. IBM, Accenture, CSC) und nachgeordnet aus Indien (z. B. infosys, wipro) beherrscht. Auch Frankreich spielt mit Capgemini eine gewisse Rolle.

Im Bereich der speziellen IT-Sicherheitsdienstleistungen sind die deutschen Anbieter *im deutschen Markt* in fast allen Untersegmenten gut vertreten (z. B. im Bereich Security Assessments, Security Strategy & Architectures sowie Zertifizierung). Diese Dienstleistungen werden häufig von kleinen, spezialisierten Firmen angeboten, finden sich aber auch im Angebotsportfolio der großen IT-Dienstleister und der Produktanbieter.

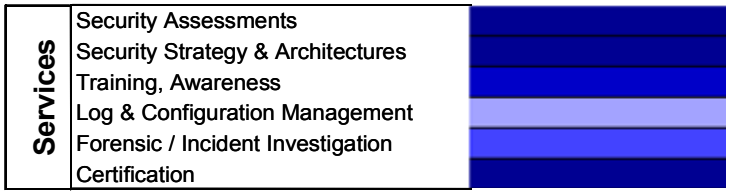


Abbildung 34: Dienstleistungs-Angebotsstruktur der IT-Sicherheitsfirmen im deutschen Markt[96]

Auch wenn somit das Kompetenzraster durch deutsche Firmen im Heimatmarkt abgedeckt wird, bleibt festzustellen, dass auf der internationalen Bühne insbesondere die einschlägigen US-amerikanischen Anbieter dominieren (u. a. die IT-Sicherheitssparten von Ernst & Young, Deloitte etc.). Eine stärkere Exportorientierung ist insbesondere für kleinere, spezialisierte Dienstleistungsunternehmen eine Herausforderung.

[96] Booz & Company Analyse

6.2 Bewertung der Ergebnisse mit Blick auf das Potential der Marktsegmente

Im Folgenden wird die herausgestellte spezifische Stärke und Marktabdeckung der deutschen Anbieter (vgl. Abschnitt 6.1) zum durchschnittlichen Wachstum und der relativen Größe des jeweiligen Segments im Weltmarkt (vgl. Abschnitt 4.5) in Beziehung gesetzt. Dadurch lassen sich besonders attraktive Bereiche identifizieren (Abbildung 35).

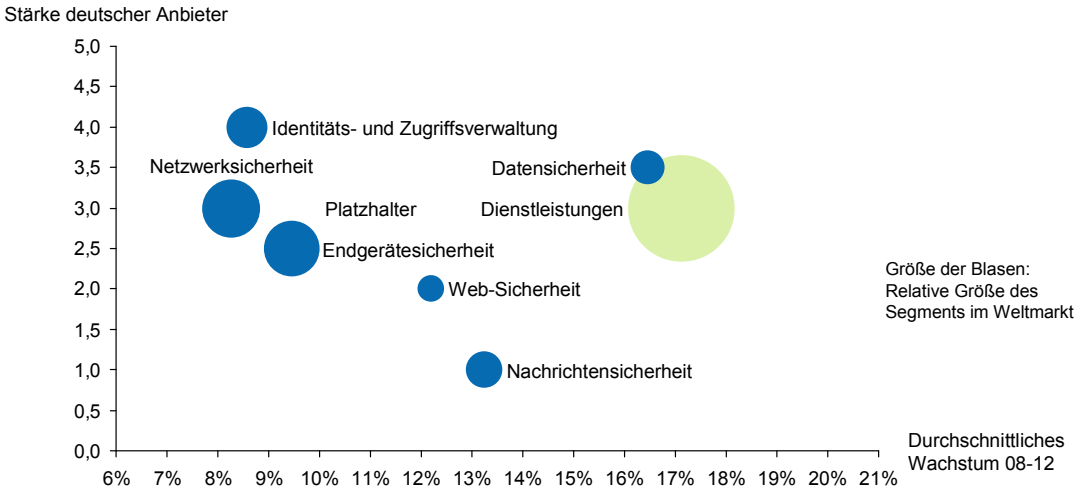


Abbildung 35: Positionierung deutscher Anbieter in den Wachstumssegmenten

Folgende Kernaussagen lassen sich daraus ableiten:

- Im Produktsegment Datensicherheit sind die deutschen Anbieter sehr gut platziert. Dabei handelt es sich zudem um das am stärksten wachsende Segment – bei allerdings noch vergleichsweise geringer absoluter Größe.
- Die klassische Stärke der deutschen Anbieter – die Identitäts- und Zugriffsverwaltung – trifft auf geringere Wachstumserwartungen als andere Segmente.
- In den Wachstumsbereichen Nachrichten- und Web-Sicherheit sind deutsche Anbieter noch (?) vergleichsweise schwach aufgestellt.
- Der Markt für Netzwerk- und Endgerätesicherheit scheint vergleichsweise gesättigt zu sein und wird zukünftig nur einstellig wachsen, wobei hier deutsche Anbieter – gerade in Nischen – gut aufgestellt sind.

- Die Dienstleistungen werden weiterhin gegenüber den Produkten an Bedeutung gewinnen. Die deutschen Anbieter sind hier jedoch bislang noch nicht optimal aufgestellt.

6.2.1 Netzwerksicherheit

Der Bereich Netzwerksicherheit ist bereits etabliert und sehr stark von Standardprodukten geprägt. Vor allem in den Untersegmenten Firewall und Virtual Private Network ist der Grad der Standardisierung bereits sehr hoch. Deutsche Anbieter existieren hier durchaus. Allerdings handelt es sich dabei meist um kleinere Unternehmen und/oder um solche, die Marktnischen gefunden und besetzt haben, wie z. B. Astaro als Anbieter von Firewall-Appliances für KMU und GeNUA als Anbieter von Firewall-Appliances im Bereich Hochsicherheit. Außerhalb von Nischen existiert nach Angaben der Anbieter mittlerweile ein Verdrängungswettbewerb, der sehr stark über die Preisgestaltung ausgetragen wird. Das Vordringen deutscher Unternehmen in die Größenordnung der Marktführer (wie Cisco, CheckPoint oder Juniper Networks) erscheint vor diesem Hintergrund wenig realistisch, andererseits wohl aber auch nicht notwendig, solange eine entsprechende Kompetenz insbesondere im Hochsicherheitsbereich in Deutschland verbleibt.

Ein größeres Potenzial für Wachstum und ggf. auch Markteintritte gibt es dagegen in den Bereichen Network Access Control und Wireless Security.

6.2.2 Endgerätesicherheit

Die Endgerätesicherheit ist ähnlich wie die Netzwerksicherheit ein relativ gesättigtes Marktsegment. Deutsche Unternehmen haben hier gewisse Stärken im Bereich Antivirus (z. B. G DATA und Avira). Obwohl diese Unternehmen technologisch durchaus konkurrenzfähig oder gar führend sind, fehlen ihnen jedoch die entsprechenden Größen- und Skaleneffekte, um Anbietern wie Symantec und McAfee in ihrer Produktvielfalt und Marktdurchdringung die Stirn zu bieten. Da der Markt weitgehend gesättigt scheint, müssen deutsche Unternehmen sich in einem Verdrängungswettbewerb gegen diese wesentlich größeren Anbieter, aber auch gegen innovative und aggressiv auftretende Fremdanbieter im deutschen Markt (wie v. a. Kaspersky) behaupten.

Ein Wachstumsbereich innerhalb der Endgerätesicherheit ist die mobile Sicherheit. Hier ist der Markt noch wesentlich weniger entwickelt, woraus sich für die deutschen Anbieter Möglichkeiten zur Expansion bzw. für Markt-

eintritte ergeben. Das entscheidende Erfolgskriterium besteht darin, ob es gelingt, die vorhandenen Kompetenzen in der Sicherheit stationärer Endgeräte zu nutzen und auf die mobile Welt zu übertragen. Nachteilig für deutsche Firmen wird sich in diesem Bereich die Tatsache auswirken, dass eine Endgeräteentwicklung und -fertigung in Deutschland kaum noch vorhanden ist.

6.2.3 Datensicherheit

Der Bereich mit dem höchsten Wachstum weltweit ist die Datensicherheit. Dies ist insbesondere dadurch zu erklären, dass sich die festen Netzwerk- und Unternehmensgrenzen auflösen, aber auch durch die steigende Bedeutung des Datenschutzes. Der Datenschutz hat in Deutschland traditionell einen hohen Stellenwert und wurde kürzlich durch eine Novellierung des Bundesdatenschutzgesetzes nochmals gestärkt.

Deutsche Firmen sind hier insbesondere im Bereich Verschlüsselung stark, z. B.:

- Rohde & Schwarz SIT und GSMK im Bereich der mobilen Verschlüsselung;
- bremen online services oder Applied Security mit Verbundprodukten, die die elektronische Signatur miteinschließen;
- Utimaco (mittlerweile im Besitz der britischen SOPHOS-Gruppe) im Bereich der Festplatten- und Dateiverschlüsselung.

In der Data Loss Prevention hingegen könnten deutsche Unternehmen stärker aktiv werden. Im Bereich Digital Rights Management liegen die Wachstumschancen für deutsche Unternehmen weniger im Medienbereich, da hier ein Trend hin zur uneingeschränkten Nutzbarkeit zu beobachten ist. Vielmehr sehen viele Marktteilnehmer im Bereich des Schutzes von Inhalten innerhalb von Unternehmen signifikante Potenziale.

Insgesamt liegen im Umfeld der Datensicherheit erhebliche Wachstumschancen für deutsche Unternehmen, da die entsprechenden Kompetenzen vorhanden sind. Die Herausforderung an dieser Stelle liegt in der Bereitstellung massenmarktfähiger Produkte, die für einen breiten Einsatz in Unternehmen und ggf. auch in Privathaushalten geeignet sind. Für den globalen Vertrieb müssten entsprechende Strukturen bzw. Partnernetzwerke etabliert werden.

6.2.4 Web-Sicherheit / Nachrichtensicherheit

Durch den ungebrochenen Siegeszug des Internets wachsen die Segmente Web-Sicherheit und Nachrichtensicherheit besonders stark. Deutsche Anbieter sind im internationalen Vergleich kaum relevant. Der Bereich Web-Sicherheit wird durch TrendMicro, Microsoft und auch McAfee dominiert, in der Nachrichtensicherheit zusätzlich noch durch Symantec.[97] Deutsche Anbieter fokussieren sich gerade auf dem Gebiet der Nachrichtensicherheit meist auf Spezialanwendungen, z. B. bremen online services im Bereich E-Government. Im Bereich der Standard-E-Mail-Kommunikation sind deutsche Anbieter lediglich in Kombination mit anderen Anwendungsfeldern am Markt präsent, z. B.

- Astaro: serverseitige E-Mail-Sicherheitsfunktionen in Verbindung mit der Firewall-Technologie;
- Avira: clientseitige Spam-Erkennung als Bestandteil der Antivirus-Software.

6.2.5 Applikationssicherheit

Die Applikationssicherheit ist ein Wachstumsfeld. Ein wesentlicher Treiber der Entwicklung ist der Trend, Aspekte der IT-Sicherheit bereits während der Anwendungsentwicklung zu berücksichtigen, statt nur die Netzwerkgrenzen abzusichern. Dadurch, dass Applikationen in zunehmendem Maße im Internet oder über mobile Netze bereitgestellt werden, kommt der Sicherstellung der Integrität dieser Applikationen eine wichtige Rolle zu. Deutsche Firmen sind in diesem Bereich als Anbieter separater Produkte noch nicht in einer signifikanten Größe präsent. Allerdings sind in diesem Umfeld Sicherheitsaspekte sehr stark in die entsprechenden Applikationen und Architekturen integriert (z. B. Sicherheitskomponenten innerhalb des Produktportfolios von SAP).

6.2.6 Identitäts- und Zugriffsverwaltung

Im Bereich der Identitäts- und Zugriffsverwaltung sind deutsche Anbieter vergleichsweise aktiv (vgl. Abschnitt 6.1). Besondere Schwerpunkte existieren in den Feldern

- Biometrie,

[97] IDC, Worldwide IT Security Software, Hardware, and Services, 2009

- Authentifizierung über Smartcards und Signaturtechnologie sowie
- Aufbau von Public-Key-Infrastrukturen (PKI).

Die Wachstumserwartungen in diesem Bereich liegen zwar unter denen für die Daten-, Web- und Nachrichtensicherheit, sind aber mit 8–9% pro Jahr durchaus attraktiv. Dieses Wachstum wird sich allerdings weniger in den Bereichen manifestieren, in denen deutsche Anbieter stark vertreten sind. Wesentliche Wachstumstreiber sind rechtliche Bestimmungen (Compliance), die den Aufbau einer unternehmensweiten Architektur für die Identitäts- und Zugriffsverwaltung fordern. Der Schwerpunkt liegt hierbei weniger auf neuen Authentisierungsmechanismen, d. h. innovativer Technologie, sondern verstärkt auf der Definition, Durchsetzung und Verwaltung entsprechender Vorgaben in Organisationen. Das Wachstum wird daher verstärkt über den Dienstleistungsbereich stattfinden und weniger in den genannten Produktfeldern.

6.2.7 Dienstleistungen

Wie bereits in Abschnitt 6.1 beschrieben, sind die deutschen Anbieter im Bereich der produktbezogenen IT-Sicherheitsdienstleistungen vorweigend auf dem nationalen Markt relevant. Dienstleistungen sind jedoch der Bereich, der innerhalb der IT-Sicherheit am stärksten wächst. Ein wesentlicher Wachstumsimpuls ist der Trend, auch den Betrieb oder gar das Management von IT-Sicherheit von externen Dienstleistern durchführen zu lassen. Obgleich der globale Markt weitgehend von den großen internationalen Anbietern beherrscht wird, ergeben sich für deutsche Anbieter im nationalen Markt durchaus Chancen. Hier sind die Kriterien „Made in Germany“ und „deutsche Eigentümerschaft“ besonders relevant. In einzelnen Nischen könnten sich auch international noch Chancen ergeben, insbesondere in Kombination mit den deutschen Stärken im Produktbereich (z. B. Hochsicherheit, Identitätsmanagement, Kryptographie).

Im Marktsegment der speziellen IT-Sicherheitsdienstleistungen ist die Situation differenziert zu betrachten:

- **Security Assessments, Strategy & Architectures:** Diese Dienstleistungen werden auch von den internationalen IT-Dienstleistern erbracht. Die Chancen für deutsche Unternehmen sind hier begrenzt.

- **Training, Awareness:** Aufgrund der Notwendigeit, die entsprechenden Maßnahmen vor Ort an die jeweilige Kultur des Landes und des Unternehmens angepasst zu erbringen, werden hier eher geringe Chancen im Export gesehen.
- **Forensic & Incident Management**: Obwohl entsprechende Kompetenz in Deutschland existiert, handelt es sich hierbei eher um einen Randbereich, der weiterhin von kleinen Anbietern mit überschaubaren Umsätzen bedient werden wird.
- **Zertifizierung**: Chancen bestehen für deutsche Anbieter insbesondere dann, wenn für die Zertifizierung profundes technologisches Know-how erforderlich ist (z. B. Zertifizierung nach Common Criteria). Zertifizierungen von Managementsystemen nach ISO-Normen sind in der Regel vergleichsweise standardisiert und können von IT-Dienstleistern vor Ort zu geringeren Kosten erbracht werden.

6.3 Zusammenfassende Beurteilung der deutschen Anbieter im Vergleich mit internationalen Wettbewerbern

Deutsche Anbieter haben in bestimmten Marktsegmenten wie Datensicherheit (Rohde & Schwarz, Utimaco) oder Identitäts- und Zugriffsverwaltung (Giesecke & Devrient) eine gute Position im Markt und mit Giesecke & Devrient auch einen Global Player. Dennoch spielen sie im internationalen Vergleich insgesamt eine eher untergeordnete Rolle. Keines der befragten Unternehmen hat im weltweiten Massenmarkt für IT-Sicherheitsprodukte (für Antivirus-Programme, standardisierte Firewalls etc.) eine annähernd vergleichbare Größenordnung erreicht wie diejenige der globalen Marktführer Symantec, McAfee, Cisco, Juniper und Checkpoint.

Im Bereich der IT-Sicherheit haben deutsche Hersteller im Ausland generell einen guten Ruf, da dieses Thema mit deutscher Ingenieurskunst und Gründlichkeit in Verbindung gebracht und bei ihnen eine verlässliche Neutralität angenommen wird. Die technologische Überlegenheit, insbesondere im Bereich der Kryptographie, sowie die Herkunftsbezeichnung „Made in Germany" sind für die deutschen Anbieter im Markt für IT-Sicherheit sehr gute Herausstellungsmerkmale.

Die folgende Tabelle gibt einen Überblick über die wichtigsten Stärken und Schwächen, die sich aus den Interviews und der Analyse der Anbieter- und Nachfragestruktur in Deutschland ergeben. Die Schwächen sind insgesamt stärker ausgeprägt und wurden nach drei wesentlichen Handlungszielen geordnet: *Sicherung kritischer Kompetenz*, *Innovation* und *Wachstum.* Unter dem Stichwort ***Sicherung*** werden die Schwächen genannt, die sich mit der Sicherung der kritischen Kompetenz sowie der kritischen Infrastruktur des Landes befassen. Das Handlungsziel ***Innovation*** umfasst alle diejenigen Schwächen, die im Zusammenhang mit dem technischen Innovationspotenzial und der Forschung bzw. Forschungsförderung stehen. Schließlich werden unter ***Wachstum*** die Schwächen zusammengefasst, die unmittelbar die Nachfrage und die Exportchancen deutscher Unternehmen betreffen.

Tabelle 12: Übersicht der wichtigsten Stärken und Schwächen des deutschen IT Sicherheitsmarkts geordnet nach Handlungszielen AUSWAHL

	Sicherung	Innovation	Wachstum
Stärken	+ Hohes Ansehen des Bundesamts für Sicherheit in der IT (BSI) + BSI-Zertifizierung international anerkannt	+ Hoher Technologiestandard + Hochwertige Fachkräfteausbildung	+ Positives Image "Made in Germany" + Hohes Vertrauen in Deutschland im Ausland + Starke Kompetenzbereiche
Schwächen	- Lücken in kritischen Kompetenzen - Keine vollständige "nationale Werkbank" - Geringe Einflussnahme auf internationale Standards	- Zu geringe Berücksichtigung internationaler Standards - Vorbildfunktion des Staates wenig ausgeprägt - Geringe Exzellenzförderung - Unklare Zielsetzung bei Großprojekten - Zu geringe Awareness	- Hoher Anteil an kleinen und mittleren Unternehmen (KMU) - Ausbaubedarf bestehender Exportunterstützung für KMU - Schwache Kooperation innerhalb der Wirtschaft - "time-to-market" zu lang - Zu hohe Abhängigkeit von Staatsaufträgen - Schwacher Kapitalmarkt

6.3.1 Stärken

Bei der Analyse der deutschen Anbieter von IT-Sicherheit (vgl. Abschnitt 5.2) sowie aus der Befragung der deutschen Anbieter im Rahmen dieser Studie hat sich der hohe Spezialisierungsgrad und die sehr **hohe technologische Kompetenz** als eine der wesentlichen Stärken der deutschen IT-Sicherheitsbranche herausgestellt. Obwohl deutsche Firmen sich schwertun, über den Status eines Nischenanbieters hinauszukommen, haben sie sich insbesondere im Hochsicherheitsbereich (z. B. secunet, Rohde & Schwarz SIT, GeNUA), bei digitalen Signaturen (z. B. KOBIL, D-Trust), Biometrie (z. B. Dermalog), Virtual Private Networks (z. B. Astaro, Sirrix), Smartcards (Giesecke & Devrient) sowie Identifizierung, ID-Management und Zertifizierungen (z. B. TÜV) gut im Markt behauptet. Im Bereich der Kryptographie wurde von einem Unternehmen ein technologischer Vorsprung von bis zu drei Jahren gegenüber ausländischen Mitbewerbern angegeben, der sogar zu erfolgreichen Geschäftsabschlüssen mit der US-amerikanischen Regierung führe. Dieser Erfolg ist auch Ausdruck des hohen Vertrauens, das Deutschland von ausländischen Regierungen entgegengebracht wird.

Deutsche Hochsicherheitsprodukte verfügen zum Teil über höchste **Sicherheitszertifizierungen** für den Einsatz im Geheimschutzbereich, z. B. RSGate (Gateway) und GeNUScreen (Firewall) von GeNUA.

Insbesondere im Mittleren Osten kommen diese Stärken sowie die Herkunftsbezeichnung „Made in Germany" zur Geltung, die auch Ausdruck

deutscher Ingenieurskunst ist. Einige Unternehmen fokussieren ihre internationalen Aktivitäten auf diese Region. So verfügt die Firma Biometrics mit 11 Mitarbeitern in Deutschland bereits über eine Tochterfirma in Abu Dhabi. Die Organisation ITSMIG e.V. (IT Security made in Germany), in der sich zahlreiche deutsche IT-Sicherheitsanbieter zusammengeschlossen haben, unterhält in dieser Region eine Marktbeobachtungsstelle, auf welche die in der ITSMIG organisierten Unternehmen zurückgreifen können.

Auch für die Inlandsnachfrage ist die hohe Kompetenz und Spezialisierung von Vorteil. So sind secunet, Mühlbauer und Rohde & Schwarz SIT Partner im Rahmen der Sicherheitspartnerschaft mit dem BMI und dienen dem BSI als „vertrauensvolle Werkbank" zur Förderung der nationaler Verschlüsselungstechnik und zur Entwicklung komplexer IT-Sicherheitslösungen im Bereich Hochsicherheit.

Selbst im Dienstleistungsbereich haben sich einige deutsche Unternehmen bereits einen Namen gemacht. So ist die TÜV Informationstechnik als eine vom BSI zugelassene Zertifizierungsstelle international erfolgreich. Dies ist auch auf das hohe Ansehen des BSI und seiner Zertifizierungen im Ausland zurückzuführen. Zudem haben sich kleine deutsche Unternehmen im Bereich der Sensibilisierung von Firmen und Mitarbeitern zum Thema IT-Sicherheit eine erfolgreiche Nische geschaffen, z. B. HECOM Security Awareness Consulting, nextsolutions, aware-house oder 8Com IT Security.

Fazit

Die deutschen Hersteller zeichnen sich durch hohe Kompetenz und Spezialisierung aus und sind insbesondere in der Hochsicherheitstechnologie erfolgreich. Die Herkunftbezeichnung „Made in Germany" ist gerade im Bereich IT-Sicherheit ein wichtiges Vertriebsargument im Auslandsgeschäft.

6.3.2 Schwächen

Aus der Analyse des IT-Sicherheitsanbieter und ihrer Rahmenbedingungen sowie aus der Befragung der Unternehmen wird deutlich, welchen Herausforderungen sich die deutsche IT-Sicherheitsbranche gegenübersieht. Dabei handelt es sich um übergreifende, strukturelle Themen, die nicht das Agieren einzelner Marktteilnehmer, sondern die heimischen Unternehmen im Bereich der IT-Sicherheit insgesamt betreffen und aus ordnungs- wie wettbewerbspolitischer Sicht auch für den Standort Deutschland insgesamt von Relevanz sind. Wie bereits dargelegt, werden diese Herausforderungen nach drei Kate-

gorien oder Handlungsfeldern geordnet: „Sicherung kritischer Kompetenz", „Innovation" und „Wachstum".

Sicherung kritischer Kompetenz

Die Sicherung kritischer Kompetenz ist eine übergeordnete Aufgabe für Deutschland als Wirtschaftsstandort und zum Schutz seiner kritischen Infrastrukturen. Wie herausgearbeitet, zeigt die deutsche IT-Sicherheitsindustrie hier empfindliche Lücken bei der notwendigen Abdeckung der gesamten Kompetenzbandbreite. Diese Situation erweist sich nicht zuletzt als eine Kehrseite der Fokussierung vieler Anbieter auf die Bereitstellung komplexer Lösungen im Hochsicherheitsbereich (gerade bei Regierungsaufträgen). Zwar ist die deutsche IT-Sicherheitstechnologie zumindest auf der EU-Ebene führend, doch wird bei der Entwicklung der Produkte vielfach zu wenig auf eine leichte Handhabbarkeit beim Einsatz im Unternehmen geachtet. Auch das BSI beklagt die starke Abhängigkeit einiger deutscher Anbieter von staatlichen Aufträgen bzw. die Tatsache, dass ihnen ein zweites Standbein fehlt.[98] Als Ausnahme sind hier Unternehmen zu nennen, die mit **standardisierten Produkten** international den Wettbewerb mit den großen Anbietern suchen, wie z. B. Astaro (Firewalls), Avira und G DATA (Virenschutz) oder auch GSMK (verschlüsselte mobile Sprachkommunikation).

Diese offene Flanke wird durch den Umstand vergrößert, dass in Deutschland wichtige Teile der IKT-Industrie vom Markt verschwunden sind. Öffentlichkeitswirksame Beispiele hierfür sind die Tatsache, dass Bosch und Siemens die Herstellung von Mobiltelefonen in Deutschland eingestellt haben, oder auch die Stilllegung der Chip-Produktion durch Qimonda. Die insgesamt stattfindende Abschmelzung wichtiger Geschäftsfelder der IKT-Industrie in Deutschland wirkt sich selbstverständlich nachteilig auf die Möglichkeit von Clusterbildungen aus. Gerade diese Cluster könnten jedoch wichtige Wachstumsimpulse setzen und sind durch die mit ihnen verbundenen „Ökoysteme" auch wichtige Innovationszentren – von denen die IT-Sicherheit als wissensintensives Feld besonders profitieren würde. Aus dieser Situation resultiert für die Regierung eine unzureichende Verfügbarkeit einer vollständigen „**vertrauensvollen Werkbank**" und damit zwangsläufig eine zunehmende Ab-

[98] Interview mit dem BSI

hängigkeit von ausländischen Herstellern. Die Chancen, diese fehlende IKT-Basisinfrastruktur in Deutschland (wieder-)aufzubauen, müssen als eher gering angesehen werden.

Insbesondere für die Entwicklung von Hochsicherheitstechnologie ist das Vertrauen in die Hersteller von hoher Bedeutung. Deutsche Anbieter besitzen somit im Heimatmarkt einen klaren Startvorteil. Und selbst im Exportgeschäft ist das Vertrauen in die Neutralität deutscher Sicherheitsprodukte – in Verbindung mit hoher technischer Leistungsfähigkeit – ein wichtiges Element, das die Wettbewerbsfähigkeit stärkt. Umgekehrt jedoch investieren andere Länder wie Korea, aber auch China, systematisch in den Aufbau ihrer **Basisinfrastruktur**, um die gesamte Wertschöpfungskette im eigenen Land abdecken zu können und so die Abhängigkeit vom ausländischen Markt im Sicherheitsbereich zu verhindern.

Der Bereich der IT-Sicherheit ist sehr stark national geprägt. Die Errichtung der Europäischen Agentur für IT-Sicherheit (ENISA) zeigt zwar erste Ansätze, das Thema IT-Sicherheit auf EU-Ebene anzugehen, doch fehlen im Gegensatz zur europäischen Verteidigungspolitik (vgl. EADS) konkrete Ansätze, um die öffentliche Beschaffung von IT Sicherheit europaweit zu koordinieren und dadurch eine europäische IT-Sicherheitsindustrie aufzubauen und zu fördern.

Innovation

Bei der Forschungsförderung im Bereich der IT-Sicherheit gibt es noch wenig ausgeprägte **Exzellenzförderung** und Kernbildung (Clusterbildung) mit dem Ziel, die Zusammenarbeit zwischen Industrie und Forschung zu verbessern und mit der internationalen Spitze mitzuhalten.

Es fehlt zudem an einer für die IT-Sicherheitsforschung wichtigen Förderung von **Risikoforschung**, bei der in raschen Entwicklungszyklen nach neuen Ansätzen und Lösungen für eine erfolgreiche Gefahrenabwehr gesucht wird. Dabei liegt es auf der Hand, dass bei einer solchen Forschung nicht aus jeder Idee eine brauchbare Lösung hervorgehen kann. Daher bringt sie auch ein hohes finanzielles Risiko mit sich, und deshalb zeigen Firmen und Forschungseinrichtungen realistischerweise ein eher geringes Interesse, sich in dieser Art von Forschung zu engagieren: Bei der derzeit übliche Förderquote von durchschnittlich 50 Prozent müssen sie ja ein erhebliches unternehmerisches Risiko selbst tragen. Tatsächlich ist die IT-Sicherheit jedoch – angesichts

der zunehmenden Bedrohung und der Professionalisierung der Angreifer – auf einen hohen Innovationsgrad angewiesen. Daher erscheint eine Förderung von bis zu 100% aus staatlichen Mitteln angemessen. (Unbestritten ist dabei allerdings, dass diese Förderquote wegen des EU-Beihilferechts nicht leicht zu realisieren sein wird.)

Ein bemerkenswertes Faktum ist, dass viele deutsche IT-Sicherheitsanbieter nur unzureichend an den Forschungsprogrammen der Regierung und der EU sowie an öffentlichen Ausschreibungen teilnehmen. Bei vielen einschlägigen Verfahren ist die Teilnahme mit Anforderungen verbunden, die einen für KMU in der Regel kaum vertretbaren Aufwand mit sich bringen. Deutschland steht zwar, was die Beteiligung und die Zuwendungen der öffentlichen Hand – z. B. aus dem abgelaufenen 6. EU Rahmenprogramm – betrifft, mit einem Anteil von 18% an der Spitze (vor Großbritannien und Frankreich). Auf die den nationalen Markt prägenden KMU entfällt dabei mit 10% der Zuwendungen für Deutschland jedoch nur ein geringer Anteil.[99]

Die deutsche Industrie sowie die IT-Sicherheitsanbieter zeichnen sich zudem durch einen eher niedrigen Grad an **Kooperation mit der Forschung** aus. In diesem Bereich zeigt beispielsweise der kanadische Mobiltelefonhersteller RIM, wie die Zusammenarbeit mit der Forschung funktionieren könnte. Unmittelbar nach Eröffnung seiner Produktionsstätte im Ruhrgebiet ist RIM auf die Universitäten und Forschungseinrichtungen in der Nähe zugegangen und hat mit diesen eine umfangreiche Kooperation vereinbart. So unterstützt das Unternehmen beispielsweise als Teil seiner Entwicklungstätigkeit Bachelorprogramme.

Negativ auf die Innovationen am Markt wirkt sich die Betrachtung der IT-Sicherheit als Compliance- und Kostenfaktor aus. Eine Folge daraus ist, dass nur das Notwendige zum Einsatz kommt, um zumindest eventuelle **Haftungsansprüche** auszuschließen. Dies ist u. a. auf eine geringe Sensibilisierung der Wirtschaft für Belange der IT-Sicherheit zurückzuführen (vgl. Abschnitt 4.3.1).

[99] ZEW, Studie für das BMBF zur deutschen Beteiligung am 6. EU Rahmenprogramm, Juli 2009

Aber auch am öffentlichen Beschaffungswesen (dem in Gestalt der Empfehlungen des BSI zur IT-Sicherheit immerhin ein Fundus an Fachwissen zur Verfügung steht) wurde in den Interviews mit den Anbieterunternehmen Kritik geübt. Durch die Vergabe entsprechender Aufträge hat der Staat nicht nur die Möglichkeit, über das Setzen von IT-Sicherheitsstandards privaten Abnehmern mit gutem Beispiel voranzugehen, sondern auch durch Generierung von Nachfrage dem Anbietermarkt für IT Sicherheitsprodukte wichtige Impulse zu geben, da öffentliche Aufträge über ihren rein finanziellen Aspekt hinaus immer auch einen referenzgebenden Charakter haben, gerade auch im IT-Sicherheitsbereich. Allerdings sind die Standardisierungs- und Zertifizierungsverfahren im IT-Sicherheitsbereich aufwendig und vor allem zeitintensiv. Damit sind sie insbesondere für die Produktpalette der den deutschen Markt prägenden KMU nur bedingt geeignet.

Schließlich haben auch Verzögerungen und eine nicht auf den Marktbedarf ausgerichtete Zielsetzung bei Leuchtturmprojekten dazu beigetragen, dass die im internationalen Vergleich zu erwartenden Wachstumspotenziale in der IT-Sicherheit nicht in vollem Umfang realisiert wurden. **Großprojekte** wie die LKW-Maut (TollCollect), die elektronische Gesundheitskarte, der elektronischer Personalausweis, und der digitaler Polizeifunk (BOS) haben einen sehr hohen **Spezifikationsgrad,** durch den ihre weitergehende Vermarktung ebenso behindert wird wie durch ihre bislang unzureichende Wechselwirkung mit der **internationalen Standardisierung.** So ist z. B. im Fall des elektronischen Personalausweises die Gültigkeit auf zehn Jahre festgelegt worden. Es ist aber nicht sichergestellt, dass die eingebaute Verschlüsselungstechnik überhaupt über einen so langen Zeitraum hinweg als sicher gelten kann.

Einen stärker auf die Marktbedürfnisse ausgerichteten Ansatz hat sich das Projekt De-Mail zum Ziel gesetzt, bei dem neben Sicherheitsaspekten (z. B. Verschlüsselung) zugleich auch die Vermarktungschancen betont werden, insbesondere mit Blick auf den Export. Erklärte Absicht ist es, dieses Projekt international zu einem Erfolgsmodell zu machen. Ein erfolgversprechender Unterschied zu den anderen Großprojekten könnte dabei in der Aufgabenverteilung zwischen der öffentlichen Hand und der Industrie liegen: De-Mail wird vorrangig von der Internetwirtschaft vorangetrieben. Der Staat konzent-

riert sich auf die Bereitstellung der Infrastruktur und den dafür benötigten Rahmen, insbesondere die rechtlichen Voraussetzungen.[100]

Wachstum

Die deutsche Anbieterlandschaft im Bereich der IT-Sicherheit zeichnet sich durch einen hohen Anteil von kleinen und mittelgroßen Unternehmen aus (vgl. Abschnitt 5.2). Die sich daraus ergebende Schwäche, Größenvorteile zu nutzen wird durch den Umstand verstärkt, dass deutsche Anbieter eine eher gering ausgeprägte Kooperationsbereitschaft zeigen. Der im Abschnitt 6.3.2 beschriebene Exodus der deutschen IKT-Industrie über die letzten Jahre verringert darüber hinaus zunehmend die Möglichkeit, Partnerschaften mit heimischen Großunternehmen zur Erzielung von Skaleneffekten und zur Erschliessung ausländischer Märkte zu schliessen.

Allerdings gibt es in Deutschland auch Positivbeispiele, bei denen kleine Produktanbieter (z. B. GeNUA, Applied Security) häufig mit Systemhäusern bzw. großen IT-Dienstleistern (z. B. T-Systems, IBM) kooperieren, um gesamthafte Lösungen anbieten zu können. Auch zwischen Produktanbietern existieren Vertriebs- bzw. Technologiepartnerschaften. So nutzt z. B. Astaro als Anbieter von Firewall Appliances die Komponente zur Entdeckung von Viren von Avira (vgl. 5.2.3).

Hinzu kommt, dass die deutschen IT-Sicherheitsanbieter aufgrund ihrer KMU-Struktur vor allem im Vergleich zu den amerikanischen Herstellern oft nicht global aufgestellt sind und demgemäß viele internationale Märkte nicht mit lokaler Präsenz bedienen können.[101]

Mittlerweile sind alle PC-Hersteller Vetriebspartnerschaften mit den großen IT-Sicherheitsanbietern wie Symantec oder McAfee eingegangen, so dass es schwer ist für deutsche Unternehmen, in diesen Massenmarkt einzudringen. Deutschen Unternehmen muss es daher gelingen, sich über ihre technologische Kompetenz gegenüber den ausländischen Anbietern zu differenzieren. Eine Differenzierung über den Preis wird wegen der hohen Standardisierung im Massenmarkt in Verbindung mit den relativ **hohen Personalkosten** in Deutschland wohl nicht gelingen. Daher sollte der Weg über die **rasche**

[100] Pilotprojekt zur Bürger-E-Post De-Mail gestartet, heise online, 8.10.2009

[101] "The European Network and Information Security Market", IDC EMEA, Schlussbericht, April 2009

Markteinführung neuer Produkte gewählt werden. Dies stellt jedoch eine besondere Schwäche derjenigen deutschen Hersteller dar, die sich auf technologisch hochwertige Produkte spezialisiert haben und die im Bereich der Hochsicherheitstechnologie Produkte und Lösungen für deutsche Behörden herstellen. Diese Produkte werden mit einem hohen Spezifikations- und Perfektionsgrad entwickelt, also in einem Prozess, der viel Zeit in Anspruch nimmt. Sie gelten dabei oft als zu kompliziert und in der Bedienung zu unhandlich. Diese Anbieter verzichten oftmals darauf, parallel an einer „zivilen" Basisversion für einen größeren und internationalen Kundenkreis zu arbeiten, die mit geringerer Spezifikation und komfortabler Benutzerführung besser und schneller zu vermarkten wäre.[102]

Die überwiegend kleinen und mittelständischen deutschen IT-Sicherheitshersteller haben es in Deutschland zudem schwer, **Kapital** für die Entwicklung neuer Produkte und die Erschließung neuer Märkte zu beschaffen. Dieses Kapital, vor allem **Wagniskapital,** ist in anderen Ländern, vor allem in den USA und Israel, viel leichter zugänglich. Deutsche Firmen haben, nachdem ihnen der **Markteintritt** gelungen ist, danach oft Schwierigkeiten, sich auf dem deutschen Markt Kapital für den Sprung ins Ausland bzw. für ein Wachstum über eine Belegschaftsgröße von 40–50 Mitarbeitern hinaus zu beschaffen. Sie wenden sich daher an risikofreudigere ausländische Investoren, für die ein Einstieg aufgrund der hochwertigen deutschen Technologie attraktiv ist, oder werden durch stärkere ausländische Anbieter übernommen, wie z. B. im Fall der Übernahme von Utimaco durch SOPHOS oder von Heimann Biometrics Systems in Jena durch Smith und später durch Cross-Match.

Auch der Staat zeigt in der Unterstützung der Unternehmen bei ihren Auslandsaktivitäten Schwächen. Nach Einschätzung der betroffenen Unternehmen dauert die Bearbeitung von **Ausfuhrgenehmigungen** in Deutschland (in Abhängigkeit vom Bestimmungsland) jedoch deutlich länger als international üblich. Die Industrie- und Handelskammer München hat auf einer Fachveranstaltung zu diesem Thema festgestellt, dass in Deutschland die Bearbeitung von Anträgen auf Ausfuhrgenehmigung im internationalen Vergleich besonders lange dauert.[103] Nach Auskunft des BAFA betrug die Bearbeitungsdauer für die Erteilung einer Einzelausfuhrgenehmigung in diesen sensitiveren Fäl-

[102] Interviews mit deutschen IT Sicherheitsunternehmen sowie Experten für IT Sicherheit

[103] Resolution des IHK-Außenwirtschaftsausschusses, IHK München, November 2006

len betrug im Jahr 2009 aufgrund der im Regelfall notwendigen Beteiligung anderer Behörden durchschnittlich 11 Wochen[104]. Eine verbindliche Festlegung einer kürzeren Bearbeitungsfrist, die den Unternehmen Planungssicherheit gäbe, fehlt bislang. Jedoch können Unternehmen ihren Beitrag dazu leisten, die Bearbeitungsdauer zu optimieren durch frühzeitige, umfassende Aufklärung des Ausfuhrsachverhalts im Unternehmen sowie eine möglichst frühzeitige Einschaltung des BAFA. So kann bereits zum Zeitpunkt der Anbahnung eines konkreten Ausfuhrgeschäfts im BAFA eine sog. Voranfrage gestellt werden, die bei positiver Bescheidung die Zusage für eine spätere Genehmigungserteilung nach Zustandekommen des Vertrags enthält.[105]

Sehr viele der befragten Unternehmen haben die USA und Frankreich auch als Beispiele für effektive **Außenwirtschaftsförderung** genannt. Insbesondere der Export von Sicherheitstechnologie erfordert Referenzprojekte und –anwendungen bei der Heimatregierung sowie eine starke Einbindung der Auslandsvertretungen, die für diesen sensiblen Bereich die notwendigen Informationen sammeln, Kontakte auf Regierungsebene vermitteln und als Referenz gegenüber dem ausländischen Käufer dienen können. Ohne starke Unterstützung durch die Regierung ist der Markt für Hochsicherheitslösungen in der öffentlicher Verwaltung und der Landesverteidigung in vielen Ländern für deutsche Firmen kaum adressierbar (z. B. Mittlerer Osten, Osteuropa).

Die deutsche Außenwirtschaftsförderung ist wegen des Prinzips der Wettbewerberneutralität durch eine starkes Eigenengagement der Wirtschaft geprägt. Außenwirtschaftsförderung erfolgt darauf aufbauend durch flankierende Maßnahmen. Im internationalen Vergleich wird das Fehlen eines darüber hinausgehenden proaktiven Dienstleistungsangebots der Botschaften z. T. von den Marktteilnehmern als Wettbewerbsnachteil empfunden. Im Bereich der IT-Sicherheit wurde daher im Jahre 2005 die (bereits mehrmals erwähnte) Exportinitiative „IT-Sicherheit made in Germany“, kurz ITSMIG e.V., gegründet. Diese bis 2008 vom BMWi finanziell getragene Initiative war insofern ein Schritt in die richtige Richtung. Allerdings hat sich der Staat mittler-

[104] Befragung von Experten des BAFA

[105] Befragung von Experten des BAFA

weile aus der unmittelbaren Förderung zurückgezogen und sich mittlerweile auf eine Schirmherrschaft beschränkt (die vom BMWi und vom BMI gemeinsam ausgeübt wird). Diese auf dem Feld der Außenwirtschaftsförderung insgesamt eher zögerliche Kooperations- und Kommunikationskultur im Verhältnis zwischen öffentlicher Hand und Wirtschaft wird von vielen Unternehmen als Schwäche im Hinblick auf ihre internationale Durchsetzungskraft bezeichnet. Andere Regierungen würden aus Sicht der befragten Anbieter mit der Wirtschaft viel partnerschaftlicher und pragmatischer umgehen und den **Staat als Unternehmer** verstehen.

Fazit

Die festgestellten Schwächen der deutschen IT-Sicherheitsbranche sind zum Teil durch die Unternehmen selbst, aber zu einem ebenso großen Teil auch durch die Rahmenbedingungen verursacht.

So könnten durch eine verbesserte Kommunikations- und Kooperationskultur zwischen den Unternehmen, der Forschung und der öffentlichen Hand eine Reihe von Schwächen behoben werden.

Die generelle Problematik der Kapitalbeschaffung über Wagniskapital oder staatliche Förderung, insbesondere bei den kleinen und mittelgroßen Unternehmen, erfordert eine größere Anstrengung.

6.4 Auswirkungen der erwarteten Marktentwicklung auf die deutschen Anbieter

Der IT-Sicherheitsmarkt ist mit einem erwarteten zweistelligen Wachstum sehr attraktiv und bietet genügend Anreize, die vorstehend beschriebenen Schwächen zu beheben und die eigenen Stärken auszubauen. Den deutschen Anbietern bieten sich viele Chancen, ihre internationale Stellung zu verbessern. Ohne ausreichende ordnungspolitische Flankierung sind die deutschen Hersteller jedoch einigen Risiken ausgesetzt, die im Anschluss kurz umschrieben werden.

6.4.1 Chancen

Eine bessere internationale Vermarktung der vorhandenen deutschen Technologie, insbesondere in Märkten, die keine eigene Kryptoindustrie haben (z. B. Indien, Singapur, Südostasien) kann erheblich dazu beitragen, ein höheres Wachstumspotenzial zu erschließen. Durch eine stärkere staatliche Begleitung und Unterstützung bei der Erschließung neuer Märkte (u. a. durch Informati-

onsbeschaffung und Kontaktvermittlung auf Regierungsebene) können die internationalen Wachstumschancen, insbesondere der KMU, noch erhöht werden. Das Label „Made in Germany“ sowie das hohe internationale Ansehen der Bundesrepublik spielen hierbei eine große Rolle und sollten bewusst eingesetzt werden.

Durch die Förderung von Firmenkooperationen sowie durch eine stärkere europäische Koordination im Hinblick auf die IT-Sicherheit (sowohl was die politische Rahmensetzung als auch was die Vergabe öffentlicher Aufträge betrifft) könnte, nicht zuletzt aufgrund der dadurch entstehenden Skaleneffekte, die Wettbewerbsposition der heimischen Anbieter gestärkt werden. In diesem Prozess haben deutsche Hersteller gute Chancen, vor allem durch ihre Kompetenzen in den Bereichen Trusted Computing, Embedded Security und Smartcards, die über einen schnelleren Time-to-market-Zyklus genutzt werden können. Die Stärke deutscher Anbieter im Bereich Embedded Security bietet Chancen bei der weiteren Entwicklung und Verbreitung der RFID-Technik und des „Internets der Dinge“.

Stärkere Kooperationen von Unternehmen mit Forschungsinstituten können die Innovationskraft stärken und zu kürzeren Entwicklungszyklen für neue, innovative Produkte führen.

Eine stärkere Beteiligung der deutschen Anbieter bei der Erarbeitung von IT-Sicherheitsstandards in den internationalen Gremien bietet ihnen zudem die Chance, ihre Kompetenzen in internationale Standards umzusetzen und somit eine stärkere Marktstellung zu erlangen, insbesondere im Ausland.

6.4.2 Risiken

Die schwache Kapitalausstattung bzw. die Schwierigkeiten bei der Kapitalbeschaffung für die überwiegend kleinen und mittelgroßen Unternehmen der deutschen IT-Sicherheitsbranche bringen das Risiko von Technologieverlust und Technologietransfer durch Marktaustritte und Übernahmen seitens ausländischer Mitbewerber mit sich.

Diese Entwicklung wird durch den weiteren Abzug der IKT-Industrie aus Deutschland (z. B. PC-Hardware) verstärkt. Hierdurch gehen inländische Kooperationsmöglichkeiten verloren und Cluster, in denen auch IT-Sicherheitsanbieter Vorteile hatten, werden aufgelöst.

Das mangelnde Bewusstsein für IT-Sicherheitsbelange und der zunehmende Einsatz von IT-Sicherheits- und Netzwerkprodukten aus dem Ausland (z. B. Switches und Router aus China) stellen aus der Sicht vieler Experten ein potenzielles Sicherheitsrisiko dar, soweit die Sicherheit bzw. „Hintertürfreiheit" dieser Produkte nicht garantiert ist.[106] So wurde der Fall der schweizerischen Crypto AG bekannt, bei dem die Firma in ihren Verschlüsselungsgeräten für Hochsicherheitsanwendungen, die in über 100 Länder verkauft wurden, eine „Hintertür" für die amerikanische National Security Agency (NSA) eingebaut haben soll.[107]

Der zunehmende Fachkräftemangel sowie die vergleichsweise hohen Personalkosten führen zur Verlagerung von Entwicklungsbereichen an ausländische Standorte (z. B. Teile der Entwicklung von Avira). Der Fachkräftemangel kann auch eine Ursache für die zu geringe Beteiligung deutscher Anbieter in internationalen Standardisierungsgremien sein. Dadurch entsteht das Risiko, dass bei wichtigen Themen im Zusammenhang mit der IT-Sicherheit die ausländische Konkurrenz den Standard bestimmt – mit der Folge, dass deren Produkte wegen ihrer höheren Standardkonformität tendenziell bevorzugt werden.

[106] Chinese backdoors "hidden in router firmware", PCPro, März 2008

[107] Ludwig De Braeckeleer, The Intelligence Daily, Dezember 2007

6.5 Priorisierung der Handlungsnotwendigkeiten

Aus der Vielzahl der aufgezeigten Stärken und Schwächen werden nun schließlich die Bereiche herausgehoben, die bei der Herausarbeitung von ordnungspolitischen Handlungsoptionen Priorität genießen sollten. Die Einteilung in die Handlungsziele Sicherung, Innovation und Wachstum wird dabei fortgeführt.

6.5.1 Sicherung: „Sicherung Nationaler Expertise“

Im Bereich der **Sicherung** kritischer Kompetenzen wird es darauf ankommen, die bestehende Kompetenz in Deutschland zum Thema IT-Sicherheit zu sichern und dort, wo Lücken erkannt werden, den Aufbau der fehlenden Expertise in Angriff zu nehmen. Zu diesem Zweck kann es sinnvoll sein, einen Kompetenz-Monitor aufzubauen und zu pflegen, der eine gezielte Förderung und Unterstützung bestehender sowie den Aufbau fehlender kritischer IT-Sicherheitskompetenzen in Deutschland ermöglicht.

6.5.2 Innovation: Forschungsförderung

Im Bereich der Innovation hat sich die fragmentierte Forschungsförderung für die IT-Sicherheit als vorrangiges Handlungsfeld herausgestellt. Die ausbaufähigen Cluster wie das Ruhrgebiet, Darmstadt, München, Berlin sollten international aufgewertet werden. Hinzu kommt die eher niedrig einzustufende Ausprägung der Anwendungs- und Risikoforschung, die auch einen Einfluss auf die geringe Bereitschaft der Industrie zur Kooperation mit der Forschung hat.

6.5.3 Wachstum: Unterstützung von KMU

Das derzeit größte Risiko für die deutsche IT-Sicherheitsbranche in ihrer aktuellen Struktur resultiert aus der Schwäche der KMU, mit Wachstums- und Vermarktungsstrategien ihre unternehmerischen Chancen im Markt zu suchen. Diejenigen jedoch, die das unternehmerische Risiko nicht scheuen, können sich nicht mit dem notwendigen Kapital für die Entwicklung neuer Produkte und Erschließung neuer Märkte zu versorgen. In diesem Bereich ist **prioritärer Handlungsbedarf**.

7 Ordnungspolitische Handlungsoptionen

In diesem Abschnitt werden aus den Erkenntnissen über die Stärken und Schwächen der deutschen IT-Sicherheitsanbieter ordnungspolitische Handlungsoptionen abgeleitet. In einem ersten Schritt werden die einschlägigen regulatorischen Rahmenbedingungen untersucht (Abschnitt 7.1). Darauf folgt ein Überblick über die wichtigsten derzeitigen Förderinitiativen auf EU-, Bundes- und Länder-Ebene (Abschnitt 7.2) sowie eine Übersicht über die Regulierungs- und Förderungspraxis in ausgewählten Ländern (Abschnitt 7.3), um so die Regulierungs- und Anreizumgebung in Deutschland im Vergleich zu anderen wichtigen internationalen Märkten zu profilieren (Abschnitt 7.4). Anschließend wird die Notwendigkeit ordnungspolitischen Handelns für die IT-Sicherheitsbranche erläutert (Abschnitt 7.5), und die herausgearbeiteten Handlungsempfehlungen werden in einer Gesamtübersicht vorgestellt (Abschnitt 7.6). Abschließend werden dann die Handlungsempfehlungen, die den Wirkungskreis des BMWi betreffen, konkretisiert (Abschnitt 7.7).

7.1 Für die IT-Sicherheit relevante rechtliche Rahmenbedingungen in Deutschland

Angesichts der vielfältigen äußeren Einflussfaktoren können ordnungspolitische Initiativen, die darauf zielen, die IT-Sicherheitsbranche zu unterstützen, nur erfolgreich sein, wenn ihnen eine genaue Analyse der bestehenden Lage vorausgegangen ist. Ein herausragender Teilbereich davon sind die rechtlichen bzw. regulatorischen Rahmenbedingungen. Denn politische Maßnahmen müssen sich ja entweder im Einklang mit bestehenden Gesetzen befinden oder aber eine Änderung der Gesetzeslage mit einschließen. Die IT-Sicherheit ist dabei von einer Vielzahl von Normen betroffen, die ganz verschiedenen Rechtsbereichen angehören.

Neben den einschlägigen EU-Vorschriften gibt es zahlreiche nationale Vorschriften (vgl. Tabelle 13), die den Bereich der IT-Sicherheit mittelbar und unmittelbar betreffen. Hierzu zählen Regelungen zum Schutz der Privatsphäre, zum Datenschutz, zum Schutz des geistigen Eigentums, zum Schutz der Vertraulichkeit, zur Transparenz, zur Exportkontrolle, zum Kampf gegen Computerbetrug und Computer- bzw. Internetkriminalität sowie Regeln zu weiteren Problemfeldern, die der Gesetzgeber zur Festlegung von Rechten und Pflichten für den sicheren Gebrauch der IT geschaffen hat. Hinzu kommen Sicherheitsstandards (ISO und Industriestandards), die die internationale IT-Gemeinde selbst als Bezugsrahmen zur Gewährleistung eines akzeptablen Sicherheitsniveaus unter den Nutzern erarbeitet hat.

Rechtliche Vorgaben können auf das IT-Sicherheitsbewusstsein bzw. –bedürfnis von Unternehmen und Verbrauchern unmittelbar oder mittelbar einwirken und damit das IT-Sicherheitsniveau beeinflussen. Sie sind daher neben der Abwehr bekannter konkreter Gefährdungen zugleich Antriebsfeder für die weltweite Nachfrage nach IT-Sicherheitsprodukten und –dienstleistungen.

Aus der Sicht der Anbieter erfüllen die heutigen Regularien in Deutschland die Aufgabe, ein angemessenes IT-Sicherheitsbewusstsein zu fördern, nicht in ausreichendem Maße.

So wies ein Unternehmen darauf hin, dass es in den Vereinigten Staaten anders als in Deutschland eine explizite Pflicht zum Schutz von Unternehmensdaten gibt, was zu einem erhöhten Sicherheitsbewusstsein und einem angemesseneren Schutzniveau beim geistigen Eigentum führt. Davon, dass sich

durch die gesetzlich stimulierte Bewusstseinsbildung das Nachfrageniveau in Bezug auf Lösungen für die Datensicherheit im Unternehmensbereich erhöht, profitiert die IT-Sicherheitsbranche gleich mehrfach, insofern sie sich anstelle der Bewusstseinsbildung auf die Sicherheitsforschung konzentrieren kann und ihre Produkte auf einem höheren allgemeinen Schutzniveau aufsetzen kann.

Andere Unternehmen kritisieren die unzureichende Transparenz im Exportkontrollverfahren in Deutschland, die durch die Einführung von verbindlichen Bearbeitungsfristen verbessert werden könnte. Ausgewogene und transparente rechtliche Vorgaben können die Unternehmen in ihren Export- und Forschungsbemühungen unterstützen.

Angesichts der Vielzahl der unmittelbar und mittelbar einschlägigen Regelungen umfasst die folgende Darstellung nur exemplarisch ausgewählte Rechtsthemen.

Die Mehrzahl der in dieser Studie untersuchten Regelungen, die mittelbar oder unmittelbar auf die IT-Sicherheitstechnologie und -industrie einwirken, sind auf die Umsetzung europäischen Rechts bzw. internationaler Abkommen und Standards zurückzuführen (z. B. Datenschutz, Forschungsbeihilfen, Exportkontrolle). Im direkten europäischen und internationalen Vergleich mit Ländern wie Frankreich, Großbritannien und den USA ist die Regelungsdichte daher durchaus vergleichbar. In den Interviews mit den Anbietern wurde allerdings durchweg die Kritik geäußert, dass bei der Umsetzung in Deutschland oftmals der Aspekt der Wirtschaftsförderung, der in der ursprünglichen Zielsetzung eine wesentliche Rolle gespielt habe, durch eine Überbetonung von Überwachungsfragen in den Hintergrund gedrängt worden sei. Auch würden internationale oder europäische Regelungen entweder „überkorrekt" oder aber noch verschärft umgesetzt.[108] Letzteres wurde einigen befragten Unternehmen z. B. bei der Zertifizierung von IT-Sicherheitsprodukten zum Wettbewerbsnachteil, da die Zertifizierung von Produkten ausländischer Konkurrenz bei ihren Heimatbehörden mit weit weniger Aufwand erfolgte.

[108] Exportkontrollrecht – Praktikablere Exportkontrolle, wirtschaft, 06/2009

Tabelle 13: Exemplarische rechtliche Regelungen

Name	Regelungsinhalt und Kernauswirkung
EU	
EG-Dual-Use-Verordnung (VO [EG] Nr. 428/2009)	Verordnung der Europäischen Union über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchfuhr von Gütern und Technologien mit doppeltem Verwendungszweck Art. 3 i. V. m. Anhang I Kategorie 5 regelt die Ausfuhrgenehmigungspflicht für bestimmte IT-Sicherheitsprodukte und -technologien, z. B. Kryptogeräte.
Bund	
Bundesdatenschutzgesetz (BDSG)	Regelungen zum Schutz personenbezogener Daten durch Behörden und Unternehmen. Im BDSG wurden die EU-Richtlinien 95/46/EG (Datenschutzrichtlinie) und 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) in nationales Recht umgesetzt. § 9 i. V. m. der Anlage zu § 9 schreibt die technischen Maßnahmen zur Sicherheit der personenbezogenen Daten vor.
Außenwirtschaftsgesetz (AWG)	Regelungen zur nationalen Ausfuhrgenehmigung, zum Exportkontrollverfahren sowie zur Wahrung der Sicherheitsinteressen der Bundesrepublik in bestimmten Schlüsselindustrien. § 7 Abs. 2 Nr. 5 regelt die Beschränkungen im Zusammenhang mit Firmenübernahmen, die deutsche IT-Sicherheitsunternehmen betreffen. § 8 i. V. m. der Ausfuhrliste regelt die Ausfuhrbeschränkungen bei bestimmten IT-Sicherheitsprodukten und –technologien, soweit diese nicht von der EU-Dual-Use-VO erfasst werden.
Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)	Artikelgesetz zur Änderung des Aktiengesetzes und zur Einführung von Risikomanagement im Unternehmensbereich. Die Vorschrift gilt unmittelbar nur für Aktiengesellschaften, aber hat eine ausstrahlende Wirkung auf andere Gesellschaftsformen wie die GmbH. § 91 Abs. 2 regelt die Pflicht zur Einführung eines internen Überwachungssystems.
Handelsgesetzbuch (HGB) Abgabenordnung (AO)	Das HGB und die AO regeln die Buchführungspflicht und die Aufbewahrung von Geschäftsunterlagen, einschließlich wichtiger Grundsätze, die den elektronischen Geschäftsverkehr und die elektronische Buchführung betreffen, insbesondere o die Grundsätze ordnungsgemäßer Speicherbuchführung (GoS), o die Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GobS) sowie o die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU). Die §§ 238 und 247 HGB sowie § 140 ff.AO regeln die

Name	Regelungsinhalt und Kernauswirkung
	Pflicht zur sicheren Aufbewahrung von Geschäftsunterlagen und schreiben die Anwendung der technischen Vorschriften der GoS, GoBS und GDPdU vor.
Bilanzrechtmodernisierungsgesetz (BilMoG)	Artikelgesetz zur Änderung des Handelsgesetzbuches und weiterer Vorschriften zur Umsetzung mehrerer EU-Richtlinien zur Corporate Governance (Abänderungsrichtlinie 2006/46/EG) und zur sog. Abschlussprüferrichtlinie 2006/43/EG § 246a Abs. 1 regelt die Pflicht zur Offenlegung der wesentlichen Merkmale des internen Kontroll- und Risikomanagementsystems.
Telekommunikationsgesetz	Das Gesetz regelt die elektronischen Informations- und Kommunikationsdienste und dient der Umsetzung der EU-Richtlinien 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) und 2006/24/EG (Vorratsspeicherung von Daten) in nationales Recht. § 109 regelt die technischen Schutzmaßnahmen für das Betreiben von Telekommunikationsanlagen.
Signaturgesetz (SigG)	Das Signaturgesetz regelt die Rahmenbedingungen und die Zertifizierung von elektronischen Signaturen. § 5 regelt die Vergabe von qualifizierten Zertifikaten und § 17 die Sicherheitsvorkehrungen in Produkten für qualifizierte elektronische Signaturen.
Telemediengesetz	Das Telemediengesetz regelt alle Teledienstleistungen, soweit diese nicht vom Telekommunikationsgesetz geregelt werden. § 13 regelt die Pflichten des Diensteanbieters zur technischen Umsetzung des Datenschutzes.
Wirtschaft	
ISO 27001	Internationaler Standard, der die Anforderungen für die Herstellung, die Einführung, den Betrieb, die Überwachung, die Wartung und die Verbesserung eines dokumentierten Informationssicherheits-Managementsystems spezifiziert.

7.1.1 Datenschutz / Datensicherheit

Ziel und Zweck des Datenschutzrechts ist es, den Einzelnen davor zu schützen, dass er durch den Umgang Dritter mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (informationelle Selbstbestimmung).

Die Einhaltung der vielfältigen Datenschutzvorschriften nimmt daher bei der Ausgestaltung und Umsetzung von IT-Sicherheitsmaßnahmen und -technologien (Datensicherheit) einen breiten Raum ein und hat eine bedeu-

tende Wirkung auf die Nachfrage nach IT-Sicherheitsprodukten und -dienstleistungen. In Deutschland hat der Datenschutz im internationalen Vergleich generell ein sehr hohes Niveau. Das Datenschutzbewusstsein in der Bevölkerung ist hoch entwickelt; insbesondere durch die Volkszählungen seit 1978 wurde die allgemeine Sensibilität für Fragen der staatlichen Erhebung und Verarbeitung von personenbezogenen Daten geschärft. Dies hat auch dazu beigetragen, dass die Umsetzung der EU-Datenschutzrichtlinie in Deutschland mehr Zeit in Anspruch nahm und erst mit sechs Jahren Verzögerung abgeschlossen wurde. Aber auch im privatwirtschaftlichen Bereich wird aufgrund der großen Zahl von Datenpannen bzw. Datenschutzverstößen (z. B. Deutsche Bahn, Deutsche Telekom, SchülerVZ) in jüngerer Zeit der Umgang mit personenbezogenen Daten kritisch verfolgt. Diese Situation verlangt von den Unternehmen verstärkte Anstrengungen bei der Einhaltung der Sicherheitsvorschriften des Datenschutzrechts.

7.1.1.1 Bundesdatenschutzgesetz (BDSG)

Das Bundesdatenschutzgesetz hat vornehmlich Behörden des Bundes sowie Unternehmen zum Adressaten. Die Bundesländer haben eigene Landesdatenschutzgesetze für ihre jeweilige Verwaltung verabschiedet.

Diese Datenschutzgesetze regeln, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig ist, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt bzw. anordnet oder der Betroffene eingewilligt hat (Verbot mit Erlaubnisvorbehalt). Bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten gilt zudem grundsätzlich das Prinzip der Datenvermeidung und der Datensparsamkeit mit dem Ziel, keine oder so wenig personenbezogene Daten wie möglich zu verwenden. Soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert, sind personenbezogene Daten darüber hinaus zu anonymisieren bzw. zu pseudonymisieren.

Das Bundesdatenschutzgesetz als allgemeine gesetzliche Vorschrift zum Datenschutz steht grundsätzlich Regelungen in spezielleren Gesetzen nach (Subsidiarität), wie zum Beispiel dem Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BSI-Gesetz).

Die später hinzugetretene EU-Datenschutzrichtlinie 95/46/EG legt einen EU-weiten Mindeststandard an Datenschutzbestimmungen fest, der im BDSG jedoch bereits umgesetzt ist.

7.1.1.2 Telekommunikationsgesetz (TKG)

Zu den Anbietern und Nachfragern von IT-Sicherheitsprodukten und -dienstleistungen in Deutschland gehören selbstverständlich insbesondere die Anbieter von Telekommunikationsdienstleistungen und Betreiber von Telekommunikationsnetzen. Diese Unternehmen fallen unter das Telekommunikationsgesetz. Angesichts der besonderen Bedeutung des Fernmeldegeheimnisses einerseits und der Verfügbarkeit von Telekommunikationsdienstleistungen für nahezu alle Lebens- und Wirtschaftsbereiche andererseits verlangt dieses Gesetz von den Betreibern von Telekommunikationsanlagen bzw. den Anbietern von öffentlichen Telekommunikationsdienstungen, angemessene Sicherheitsvorkehrungen zu treffen und hierüber durch Vorlage eines Sicherheitskonzepts gegenüber der Bundesnetzagentur als Aufsichtsbehörde Rechenschaft abzulegen (§ 109 TKG). Das gilt z. B. auch und insbesondere für die im Zuge der sogenannten Vorratsdatenspeicherung von allen Telekommunikationsanbietern zu speichernden Datensätze.

Die Bundesnetzagentur erstellt nach § 109 TKG als Richtschnur für das Sicherheitskonzept der Unternehmen einen Katalog von Sicherheitsanforderungen für den Betrieb von Telekommunikations- und Datenverarbeitungssystemen erstellt. Er soll angemessene Sicherheitsvorkehrungen auf dem neuesten Stand der Technik und im Einklang mit den geltenden internationalen Maßstäben gewährleisten.

7.1.1.3 Telemediengesetz

Das Telemediengesetz befasst sich mit elektronischen Informations- und Kommunikationsdiensten, soweit sie nicht Telekommunikationsdienste oder telekommunikationsgestützte Dienste im Sinne des Telekommunikationsgesetzes sind oder Rundfunk nach dem Rundfunkstaatsvertrag darstellen. Zweck des Gesetzes ist es, Telemedien von in der Bundesrepublik Deutschland niedergelassenen Diensteanbietern den Anforderungen des deutschen Rechts zu unterwerfen (u. a. Datenschutz), und zwar auch dann, wenn die Telemedien in einem anderen Staat des europäischen Binnenmarkts geschäftsmäßig angeboten bzw. die entsprechenden Leistungen erbracht werden.

Telemedien, die in der Bundesrepublik Deutschland von Diensteanbietern geschäftsmäßig angeboten werden, die in einem anderen Staat innerhalb des europäischen Binnenmarktes niedergelassen sind, sind nicht Gegenstand des Telemediengesetzes.

Das Telemediengesetz betrifft die IT-Sicherheit insofern, als es vom Diensteanbieter die Speicherung und die Gewährleistung der Sicherheit von Bestands- und Nutzungsdaten fordert, den Personenkreis, der üblicherweise die Herausgabe personenbezogener Daten verlangen kann, um die Geheimdienste und den Urheberrechtsinhaber erweitert sowie die Versendung von Spam-E-Mails zur Ordnungswidrigkeit erhebt.

7.1.2 Gesellschaftsrecht

Im Gesellschaftsrecht ist die Frage nach dem Umfang der Absicherung der IT-Systeme mit der Frage nach dem Umfang der Haftung des Unternehmens im Schadensfall verknüpft. Sicherheit und Schutz des technischen und wirtschaftlichen Know-hows liegen vorrangig in der Eigenverantwortung jedes Unternehmens.[109] Damit wird der Schutz von IT-Systemen eine organisatorische Grundentscheidung des Unternehmens.

Explizite IT-Sicherheitsstandards oder eine ausdrückliche IT-Basissicherung enthalten die Vorschriften nicht. Da IT-Sicherheitsrisiken zumeist nicht sichtbar oder physisch greifbar sind, setzt ihre Einschätzung detaillierte Kenntnisse der eigenen IT und der äußeren Bedrohung voraus, die den verantwortlichen Entscheidern oftmals fehlen. Gleichwohl sind die Probleme in den Unternehmen bekannt. So gab in einer für das BMWi durchgeführten Befragung von etwa 250 kleinen und mittelständischen Unternehmen durch das E-Commerce Center Handel im Jahre 2008 nur jedes fünfte Unternehmen an, während der letzen 12 Monate durch IT-Ausfall in der täglichen Arbeit unterbrochen worden zu sein (vgl. die folgende Abbildung).

[109] Hintze, IT-Sicherheit und der Schutz vor Computerkriminalität als Wirtschaftsfaktor, Januar 2009

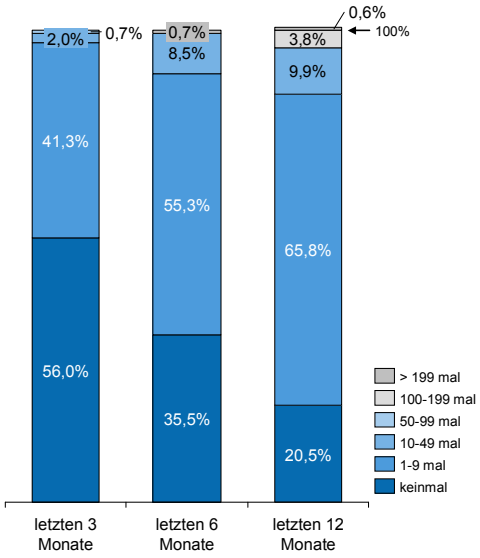


Abbildung 36: Unterbrechung der täglichen Arbeit durch IT-Probleme[110]

In Ermangelung gesetzlicher Vorgaben zur IT-Basissicherung und aufgrund der mit IT-Sicherheit verbundenen Kosten kommt in Unternehmen meist nur so viel IT-Sicherheit zum Einsatz, wie unter Haftungsaspekten zwingend erforderlich erscheint. Ein solches Risikomanagement führt nicht selten dazu, dass nicht ausreichend gesicherte Systeme verwendet oder bekannt gewordene Sicherheitslücken nicht geschlossen werden. Die folgenden Gesetze und Vorschriften regeln das Risikomanagement in Unternehmen und die Pflicht zur Veröffentlichung in Geschäftsberichten.

7.1.2.1 Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

Übergreifende rechtliche Vorgaben zum Risikomanagement, d. h. zum kontrollierten Umgang mit Risiken und Krisen, wurden 1998 für Kapitalgesellschaften wie die Aktiengesellschaft (AG), die Kommanditgesellschaft auf Aktion (KGaA) und große Gesellschaften mit beschränkter Haftung (GmbH) durch das **Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)** eingeführt. Das KonTraG fordert ein Überwachungssystem, welches alle existenzgefährdenden Risiken eines Unternehmens umfasst, d. h. neben Marktrisiken auch Natur- und Sicherheitsrisiken. Hierunter fallen insbesondere die IT-Risiken, da diese den Fortbestand der Gesellschaft ernsthaft gefährden können.

[110] ECC, Informationssicherheit in Unternehmen 2008, Oktober 2008

Für die Kreditwirtschaft sowie für die Versicherungswirtschaft gelten die Bestimmungen des Kreditwirtschaftsgesetzes (KWG) bzw. des Versicherungsaufsichtsgesetzes (VAG), auf deren Grundlage die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) im Rahmen ihrer Aufsicht verpflichtende **Mindestanforderungen an das Risikomanagement (MaRisk)** erlassen hat, die in regelmäßigen Abständen aktualisiert werden.

Die MaRisk stellen konkrete Anforderungen an die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten in den IT-Systemen (Hardware- und Software-Komponenten) und den zugehörigen IT-Prozessen. Die MaRisk verweisen lediglich auf gängige Standards wie beispielsweise das IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und den internationalen Sicherheitsstandard ISO/IEC 27002 der International Standards Organization (ISO), ohne diese verpflichtend vorzuschreiben.

7.1.2.2 Bilanzrechtmodernisierungsgesetz (BilMoG)

Das **Bilanzrechtmodernisierungsgesetz (BilMoG)** hat die Offenlegungspflichten für Publikumsgesellschaften erweitert. Von Unternehmen wird gefordert, die wesentlichen Merkmale des internen Kontrollsystems und des Risikomanagementsystems im Hinblick auf den Rechnungslegungsprozess im (Konzern-)Lagebericht zu beschreiben. Durch diese Änderungen wurden europarechtliche Vorgaben der 4. und 7. gesellschaftsrechtlichen Richtlinien sowie der 8. gesellschaftsrechtliche Richtlinie (2006/43/EC), auch Abschlussprüferrichtlinie oder Euro-SOX-Richtlinie genannt, in nationales Recht umgesetzt.

7.1.2.3 Handelsgesetzbuch (HGB) und Abgabenordnung (AO)

Das Handelsgesetzbuch und die Abgabenordnung regeln die Buchführungspflichten und die Pflichten zur Aufbewahrung von Geschäftsunterlagen und legen insbesondere Grundsätze für die Aufbewahrung des elektronischen Geschäftsverkehrs und für die Durchführung der elektronischen Buchführung fest. Hierzu zählen insbesondere

- die Grundsätze ordnungsgemäßer Speicherbuchführung (GoS),
- die Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GobS) sowie

- die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU).

Diese Grundsätze stellen wichtige Anforderungen an die IT-Sicherheit der gewählten Datenspeicherungs- und -archivierungssysteme zur Gewährleistung der Verfügbarkeit und Integrität der abgespeicherten Daten.

7.1.3 Sicherheitsstandards und Zertifizierung

7.1.3.1 BSI-Gesetz

Mit dem Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes wird dem Bundesamt für Sicherheit in der Informationstechnik (BSI) die Befugnis eingeräumt, technische Vorgaben für die Sicherung der Informationstechnik in der Bundesverwaltung zu machen und Maßnahmen zu ergreifen, um Gefahren für die Sicherheit der Informationstechnik des Bundes abzuwehren. Laut Koalitionsvertrag der neuen Bundesregierung soll das Bundesamt für Sicherheit in der Informationstechnik zur zentralen Cyber-Sicherheitsbehörde ausgebaut werden, um vor allem die Abwehr von IT-Angriffen koordinieren zu können. Im Folgenden wird auf die Rolle des BSI als Berater und Dienstleister der Bundesverwaltung sowie auf seine Rolle als nationale Zertifizierungsstelle eingegangen.

Berater und Dienstleister für den Bund

Das BSI hat Standards für den IT-Grundschutz auf der Basis des internationalen ISO Standards 27001 erarbeitet. Diese BSI-Standards enthalten Empfehlungen des BSI zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit, auf die hier im Detail nicht näher eingegangen werden soll. Das BSI greift dabei Themenbereiche auf, die von grundsätzlicher Bedeutung für die Informationssicherheit in Behörden oder Unternehmen sind und für die sich national oder international sinnvolle und zweckmäßige Herangehensweisen etabliert haben.

Die BSI-Standards dienen zwar in erster Linie der fachlichen Unterstützung von Behörden und Unternehmen, die die Empfehlungen des BSI nutzen und an ihre eigenen Anforderungen anpassen können.[111] Aber auch Hersteller von

[111] Für die öffentlichen Stellen des Bundes (Behörden, Körperschaften, Anstalten, Stiftungen oder andere juristische Personen des öffentlichen Rechts) kann das Bundesministerium des Innern nach Zustimmung des Rats der IT-Beauftragten der Bundesregierung die vom BSI er-

Informationstechnik oder Dienstleister können auf die Empfehlungen des BSI zurückgreifen, um ihre Angebote sicherer zu machen.

Wie bereits beim Gesellschaftsrecht (7.1.2) ausgeführt, gibt es für Unternehmen der Kredit- und Versicherungswirtschaft Anforderungen im Rahmen des gesetzlich vorgeschriebenen Risikomanagements, IT-Sicherheitstandards wie die ISO 27001 anzuwenden.

Das BSI-Gesetz sieht die Möglichkeit vor, BSI-Mindeststandards für die Bundesbehörden vorzuschreiben. Damit wird die Rolle des Staates als Vorreiter und Vorbild unterstrichen, eine Funktion, die auch eine unmittelbare Wirkung auf die Nachfrage nach IT-Sicherheit mit sich bringt. Ab 2010 wird darüber hinaus auch dem neu geschaffenen IT-Planungsrat von Bund, Ländern und Kommunen die Möglichkeit gegeben, Standards für die Interoperabilität und Sicherheit im IT-Bereich festzulegen.[112]

Das BSI als nationale Zertifizierungsstelle

Das Bundesamt für Sicherheit in der Informationstechnik ist auch die nationale **Zertifizierungsstelle** der Bundesverwaltung für IT-Sicherheit. Nach dem **BSI-Gesetz** erteilt das BSI das deutsche IT-Sicherheitszertifikat.[113] Das BSI führt verschiedene Zertifizierungen durch:

- Zertifizierung von Produkten (Systeme oder Komponenten) der Informationstechnik auf Veranlassung des Herstellers oder Vertreibers
- Bestätigungen für Produkte gemäß Signaturgesetz (§ 15 Abs. 7 S. 1 bzw. § 17 Abs. 4)
- Zertifizierung nach Technischen Richtlinien (TR) u. a. für IT-Produkte und -Systeme, die für den Einsatz in hoheitlichen, sicherheitskritischen Bereichen der Bundesrepublik Deutschland vorgesehen sind und bei

---

arbeiteten Standards ganz oder teilweise als allgemeine Verwaltungsvorschriften erlassen. Für Gerichte und Verfassungsorgane haben diese Vorschriften nur empfehlenden Charakter.

[112] „Föderalismusreform in Kraft", Pressemitteilung vom 5.8.2009, Deutschland Online

[113] Neben der Erfüllung der vom BSI festgelegten Kriterien hängt die Erteilung eines BSI-Sicherheitszertifikats für Personen, IT-Sicherheitsdienstleister, informationstechnische Systeme, Komponenten, Produkte oder Schutzprofile bzw. die Anerkennung als sachverständige externe Prüfstelle von der Feststellung des Bundesministeriums des Innern (BMI) ab, dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, dem nicht entgegenstehen.

denen besondere Anforderungen u. a. an die elektronische Fälschungssicherheit, Betriebszuverlässigkeit oder Interoperabilität gestellt werden

- IT-Grundschutzzertifikate für Personen, Unternehmen und Behörden nach dem internationalen Standard ISO 27001
- Akkreditierung externer Prüfstellen, insbesondere von Auditoren, Evaluatoren, Prüfern, Lauschabwehr- und Abstrahlprüfstellen.

Diese (nationalen) Zertifikate haben auch international eine große Bedeutung. Zur Vermeidung von Mehrfach-Zertifizierungen des gleichen Produktes in verschiedenen Staaten, wurde international unter Beachtung gewisser Bedingungen eine gegenseitige Anerkennung von IT-Sicherheitszertifikaten – auf der Basis der Common Criteria (CC) der IT-SEC – vereinbart. Sicherheitszertifikate anderer anerkannter Zertifizierungsstellen aus dem Bereich der Europäischen Union werden vom BSI gemäß § 9 Abs. 7 des BSI-Gesetzes anerkannt, soweit sie eine den Sicherheitszertifikaten des Bundesamtes gleichwertige Sicherheit ausweisen und die Gleichwertigkeit vom Bundesamt festgestellt worden ist. Grundlage hierfür ist zum einen das im März 1998 in Kraft getretene Abkommen über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten (SOGIS-MRA) bis zur Evaluationstufe 7. Das Abkommen wurde bislang von 9 EU-Staaten und Norwegen unterzeichnet, das BSI erkennt jedoch bislang nur die Zertifikate der nationalen Zertifizierungsstellen Frankreichs und Großbritanniens und seit Januar 2009 auch der Niederlande an. Des Weiteren gibt es die Common-Criteria-Vereinbarung über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten und -Schutzprofilen auf Basis der CC bis einschließlich der Vertrauenswürdigkeitsstufe EAL 4 (CC-MRA). Dieser Vereinbarung sind bislang 26 Staaten beigetreten (einschließlich der USA, aber bislang ohne China).[114]

IT-Sicherheitsprodukte (vor allem Kryptosysteme), die für die Verarbeitung und Übertragung von Verschlusssachen (Streng Geheim, Geheim, VS-Vertraulich und VS-Nur für den Dienstgebrauch) im Bereich des Bundes und der Länder eingesetzt werden sollen, müssen oder sollen gemäß Verschlusssachenanweisung des BMI vom BSI zugelassen sein. In der Regel kommen

[114] www.bsi.bund.de – Zertifizierung nach IT-SEC und CC

dabei Produkte zum Einsatz, die nach Common Criteria mit nationalem Schutzprofil durch das BSI zertifiziert wurden.

7.1.3.2 Signaturgesetz (SigG)

Das deutsche Signaturgesetz legt Rahmenbedingungen für elektronische Signaturen fest und regelt die Zertifizierung von elektronischen Unterschriften. Die Anwendung einer elektronischen Unterschrift ist freiwillig, soweit die Anwendung nicht per Gesetz vorgeschrieben wird.

In Deutschland ist seit dem 1. Januar 2002 gemäß dem Umsatzsteuergesetz (UStG) für elektronische Rechnungen die strengste Stufe der elektronischen Unterschrift erforderlich, die qualifizierte elektronische Unterschrift. Diese strenge Anforderung wurde seinerzeit mit der Bekämpfung des Umsatzsteuerbetruges begründet. Die Regelung im Umsatzsteuergesetz beruht auf der Mehrwertsteuerrichtlinie der EU (2001/115/EC).

Die Europäische Kommission hat mittlerweile erkannt, dass die Regeln zur elektronischen Rechnungsstellung zu kompliziert seien, in der EU zu unterschiedlich angewendet würden und folglich die Verbreitung des grenzüberschreitenden elektronischen Geschäftsverkehrs einschließlich der elektronischen Rechnung behinderten. Als Teil eines Aktionsplans der Kommission, die Bürokratie für die Unternehmen in der EU bis 2012 um 25 Prozent abzubauen, wurde die Änderung der Regelung über elektronische Rechnungen als einer von insgesamt 42 Rechtsakten ausgewählt, mit denen die EU dieses Ziel erreichen will. Anfang 2009 hat die EU-Kommission eine Änderung der Mehrwertsteuerrichtlinie beschlossen, um diese Regeln zu lockern.

7.1.4 Exportkontrolle und Technologietransfer

IT-Sicherheitsprodukte und -technologien können Ausfuhrbeschränkungen unterliegen. Hersteller, die ihre Produkte und Dienstleistungen ins Ausland liefern wollen, müssen sich daher über die Vorschriften zur Ausfuhrkontrolle, insbesondere das Außenwirtschaftsgesetz, im Klaren sein.

Generell gilt, dass der Waren-, Dienstleistungs-, Kapital-, Zahlungs- und sonstige Wirtschaftsverkehr mit fremden Wirtschaftsgebieten (Außenwirtschaftsverkehr) grundsätzlich frei ist. Nach § 7 des Außenwirtschaftsgesetzes (AWG) sind aber Beschränkungen möglich, um

- die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland zu gewährleisten,

- eine Störung des friedlichen Zusammenlebens der Völker zu verhüten oder
- zu verhüten, dass die auswärtigen Beziehungen der Bundesrepublik Deutschland erheblich gestört werden.

Kontrolliert wird der Außenwirtschaftsverkehr mit strategisch wichtigen Gütern, vor allem Waffen, Rüstungsgütern und Gütern mit doppeltem Verwendungszweck (sog. **Dual-Use-Güter**). Güter mit doppeltem Verwendungszweck sind Waren, Software und Technologie, die für zivile und militärische Zwecke verwendet werden können. Im Bereich der Software trifft dies vor allem auf Kryptoprodukte zu.

Neben den nationalen Vorschriften sind die Exportkontrollvorschriften der Europäischen Union (EU) zu beachten. Die Verordnung (EG) Nr. 428/2009 des Rates vom 5. Mai 2009 über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung und der Durchfuhr von Gütern und Technologien mit doppeltem Verwendungszweck (nachfolgend „EG-Dual-Use-VO“) legt für alle Mitgliedstaaten der EU eine einheitliche Güterliste (Anhang I zur EG-Dual-Use-VO) und Genehmigungspflichten sowie -verfahren für die Ausfuhr und Verbringung von Dual-Use-Gütern verbindlich fest.

Für die IT-Sicherheitsbranche ist es besonders wichtig, dass die Übertragung von Software oder Technologie mittels elektronischer Medien wie Telefax, Telefon, elektronischer Post oder sonstiger elektronischer Träger in ein Bestimmungsziel außerhalb der Europäischen Gemeinschaft eine Ausfuhr ist. Hierzu zählt auch das Bereitstellen solcher Software oder Technologie in elektronischer Form (sogenannter „Upload“) für juristische oder natürliche Personen oder Personenvereinigungen außerhalb der Gemeinschaft. Als Ausfuhr gilt außerdem die mündliche Weitergabe von Technologie, wenn die Technologie am Telefon beschrieben wird.

Neben den **Einzelgenehmigungen** gibt es für einen großen Kreis von Waren und Technologien allgemeine Genehmigungen, die eine wesentliche Verfahrenserleichterung darstellen. **Allgemeine Genehmigungen** haben die gleiche Wirkungen wie alle anderen Ausfuhrgenehmigungen, müssen aber nicht beantragt werden. Allgemeine Genehmigungen werden von Amts wegen bekannt gegeben und bewirken, dass alle Ausfuhren, die die Voraussetzungen der jeweiligen allgemeinen Genehmigung erfüllen, genehmigt sind.

Für die IT-Sicherheitsbranche von besonderer Bedeutung ist die **allgemeine Genehmigung Nr. EU001**. Die allgemeine Genehmigung Nr. EU001 gilt nur für Ausfuhren von Gütern des Anhangs I der EG-Dual-Use-VO[115] (z. B. kerntechnische Materialien, Elektronik, PCs, Telekommunikation, Laser, Güter der Luft- und Raumfahrtechnik usw.) nach Australien, Japan, Kanada, Neuseeland, Norwegen, in die Schweiz und die Vereinigten Staaten von Amerika. Sie gilt nicht für Ausfuhren von bestimmten Gütern der „Kryptotechnik", die zu den Gütern der gemeinschaftlichen strategischen Überwachung zählen. Eine genaue Beschreibung der unter „Kryptotechnik" fallender Güter ist im Anhang I Kategorie 5 Teil 2 der Dual-Use-VO enthalten.

Neben der allgemeinen Genehmigung Nr. EU001, die immer vorrangig zu verwenden ist, gibt es die nationale allgemeine Genehmigung Nr. 16 (Telekommunikation und Informationssicherheit).

Für die Inanspruchnahme von allgemeinen Genehmigungen gilt ein generelles einmaliges Registrierverfahren, welches bis spätestens 30 Tage nach der ersten Ausfuhr durchgeführt sein muss. Für die allgemeine Genehmigung Nr. 16 gilt jedoch ein erweitertes Registrierverfahren, welches neben dem Registrierungsformular die Vorlage einer Liste der Länder und Güter erfordert, die mit der allgemeinen Genehmigung Nr. 16 ausgeführt werden sollen.

Zuverlässige Ausführer, die in erheblichem Umfang am Außenwirtschaftsverkehr teilnehmen, können zudem am vereinfachten Verfahren der sogenannten Sammelausfuhrgenehmigungen teilnehmen. Mit dieser Form der Genehmigung werden vom BAFA eine Vielzahl von Ausfuhrvorgängen an eine Vielzahl von Empfängern innerhalb eines festgelegten Zeitraums genehmigt.

Das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) ist in Deutschland für die Prüfung der Genehmigungsfähigkeit und für die Erteilung der Ausfuhrgenehmigung zuständig.

Besonders komplex sind die rechtlichen und administrativen Probleme bei der Genehmigung von Dual-Use-Gütern. Nach Angaben des BAFA haben Güter mit doppeltem Verwendungszweck den weitaus größten Anteil an den

[115] Vgl. www.ausfuhrkontrolle.info/ausfuhrkontrolle/de/gueterlisten/-anhaenge_egdualusevo/index.html

Ausfuhren, die jährlich die Grenzen überschreiten, wobei ihr Verwendungszweck in der Regel nicht unmittelbar erkennbar ist.[116]

Das BAFA trifft die Entscheidung über die Genehmigung bzw. Ablehnung unter Berücksichtigung aller zur Verfügung stehenden Informationen über den beabsichtigten Verwendungszweck. In einer Reihe von Fällen trifft das BAFA die Entscheidung erst nach politischer Abwägung durch das Bundesministerium für Wirtschaft und Technologie (BMWi) und das Auswärtige Amt.[117] Zudem wird bei manchen dieser Produkte auch das Bundesamt für Sicherheit in der Informationstechnik im Genehmigungsverfahren beteiligt.

Gemäß statistischer Auswertung des BAFA für das Jahr 2009 betrug der Anteil der Ausfuhrgenehmigungen für Waren und Software, die dem Bereich der IT-Sicherheit im Dual-use-Sektor zugeordnet werden können, ca. 2 % an der Gesamtzahl der für gelistete Dual-use-Güter erteilten Ausfuhrgenehmigungen. Von dieser Zahl nicht erfasst sind die Ausfuhren, die unter Inanspruchnahme der zuvor beschriebenen allgemeinen Genehmigungen getätigt wurden.[118]

Mit der Novellierung der Dual-Use-VO im Mai 2009 wurden Bearbeitungsfristen für das Genehmigungsverfahren in den Verordnungstext aufgenommen. Jedoch stellt Art. 10 Abs. 3 der Dual-Use-VO die Festlegung dieser Frist in das Ermessen der einzelnen Mitgliedstaaten, das unter Berücksichtigung der einzelstaatlichen Rechtsvorschriften und Gepflogenheiten ausgeübt werden soll. Nach Auskunft des BAFA, wird die Bundesrepublik von der Möglichkeit der Einführung einer Bearbeitungsfrist für die Erteilung von Ausfuhrgenehmigungen keinen Gebrauch machen.[119]

7.1.5 Öffentliche Auftragsvergabe

Die öffentliche Verwaltung ist ein bedeutender Abnehmer von IT-Sicherheitsprodukten und -dienstleistungen. Allerdings muss sie nach den Haushaltsgesetzen das Prinzip der Wirtschaftlichkeit beachten und sich bei der Verwendung der Steuergelder an formelle Verfahren halten.

---

[116] Siehe www.ausfuhrkontrolle.info/ausfuhrkontrolle/de/aufgaben/index.html

[117] Bundesamt für Wirtschaft und Ausfuhrkontrolle, Jahresbericht 2008, Januar 2009

[118] Befragung von Experten des BAFA

[119] Befragung von Experten des BAFA

Vorrangig sind die öffentlichen Auftraggeber zur öffentlichen Ausschreibung (bzw. dem offenen Verfahren) verpflichtet, da es den potenziell größten Wettbewerb organisiert. Für die Hersteller von IT-Sicherheit im Hochsicherheitsbereich, z. B. für den Geheimschutz, ist es wichtig, dass Beschaffungen, die für geheim erklärt werden bzw. besondere Sicherheitsmaßnahmen erfordern, gemäß Art. 14 der EG-Lieferkoordinierungsrichtlinie von der Anwendung dieser EG-Richtlinie ausgenommen sind. Diese Beschaffungen können im Wege der beschränkten Ausschreibung erfolgen und auf einen geographischen Anwendungsbereich (z. B. Deutschland) beschränkt werden.

Zur Verbesserung der Teilnahmebedingungen für KMUs hat die Bundesregierung das Vergaberecht mit dem Gesetz zur Modernisierung des Vergaberechts vom 21. April 2009 modernisiert. Die Änderungen insbesondere zu § 97 des **Gesetzes gegen Wettbewerbsbeschränkungen** sehen vor, dass mittelständische Interessen bei der Vergabe öffentlicher Aufträge zu berücksichtigen sind. Insbesondere sind Leistungen nach Menge (Teillose) und Art (Fachlose) getrennt zu vergeben. Darüber hinaus sind weitere qualifizierende Aspekte zu beachten: So sind Aufträge an fachkundige, leistungsfähige sowie gesetzestreue und zuverlässige Unternehmen zu vergeben. Außerdem können Anforderungen an Auftragnehmer gestellt werden, die soziale, umweltbezogene und innovative Aspekte betreffen, wenn sie im sachlichen Zusammenhang mit dem Auftragsgegenstand stehen.

Mit Bezug auf die Beschaffung von IT-Sicherheitsprodukten stellt das BSI im Rahmen seiner Aufgaben **technische Richtlinien** bereit. Diese sind (neben den vergaberechtlichen Vorschriften) von den Dienststellen des Bundes bei der Entwicklung sachgerechter Anforderungen an Auftragnehmer (Eignung) und IT-Produkte (Spezifikation) zu berücksichtigen. Diese Richtlinien beinhalten Vorschriften zur Feststellung der Eignung der Anbieter und der angebotenen Leistungen aus Sicht der IT-Sicherheit. Das BSI kann zudem auf die Nachfrage von bestimmten IT-Sicherheitsprodukten (z. B. Virenscanner, Firewalls, Verschlüsselungstechnik usw.) Einfluss nehmen und diese für den Bund bereitstellen. Die Abnahme kann durch Beschluss des Rats verpflichtend gemacht werden.

7.1.6 Rechtliche Grundlagen für die staatliche Förderung von Forschung und Entwicklung

Die staatliche Förderung von Forschung und Entwicklung (FuE) ist für die IT-Sicherheitsbranche von großer Bedeutung. Aus der Befragung der Unternehmen und Forschungseinrichtungen im Rahmen dieser Studie haben sich einige Fragestellungen ergeben, die eine nähere Betrachtung der rechtlichen Grundlagen der staatlichen Förderung von FuE-Vorhaben notwendig machen. Dabei steht besonders auch die Frage im Hintergrund, wie eventuelle staatliche Handlungsoptionen im Hinblick auf ihre (EU-)rechtliche Zulässigkeit einzuschätzen sind.

Staatliche Fördermittel stellen grundsätzlich eine Beihilfe nach den EU-Vorschriften dar. In der EU gilt jedoch grundsätzlich ein Beihilfeverbot, da Beihilfen von staatlicher Seite gemäß Art. 87 des EG-Vertrages als nicht mit dem freien Binnenmarkt vereinbar angesehen werden. Ausnahmen von dieser Regel hat die EU-Kommission in einem Gemeinschaftsrahmen mit klar definierten Maßnahmen für FuE festgelegt. Alle national vereinbarten Förderprogramme müssen als eine der im Gemeinschaftsrahmen genannten Maßnahmen definiert sein und die übrigen Bedingungen des Gemeinschaftsrahmens erfüllen, damit die EU-Kommission diese Förderung als mit dem EG-Vertrag vereinbar genehmigen kann. Dies trifft vor allem auf die Höhe der öffentlichen Zuwendung zu, die abhängig von der Fördermaßnahme begrenzt ist. Die für die IT-Sicherheitsforschung wesentlichen Maßnahmen sind:

1. Beihilfen für Vorhaben im Bereich der Grundlagen- und der industriellen Forschung sowie der experimentellen Entwicklung,

2. Beihilfen für technische Durchführbarkeitsstudien,

3. Beihilfen für junge innovative Unternehmen,

4. Beihilfen für Innovationskerne bzw. Cluster.

Neben den Unternehmen fallen auch Forschungseinrichtungen unter das EU-Beihilferecht. Demnach sind Förderungen mit dem EG-Vertrag dann vereinbar, wenn sich die Förderung ausschließlich auf die nicht-wirtschaftliche Tätigkeit der Forschungseinrichtung bezieht und die wirtschaftliche von der nicht-wirtschaftlichen Tätigkeit mit Blick auf Kosten und Finanzierung eindeutig getrennt werden kann.

Die folgende Tabelle gibt einen exemplarischen Überblick über die maximal zulässige Förderquote einschließlich möglicher Zuschläge:

Tabelle 14: Übersicht zur maximal zulässigen Förderquoten für FuE-Vorhaben

Forschungskategorie	Kleine Unternehmen	Mittlere Unternehmen	Große Unternehmen
Grundlagenforschung	100 %	100 %	100 %
Industrielle Forschung	70 %	60 %	50 %
Kooperationen	80 %	75 %	65 %
Experimentelle Entwicklung	45 %	35 %	25 %
Kooperationen	60 %	50 %	40 %
Durchführbarkeitsstudien			
- industrielle Vorhaben	75%	75%	60%
- experimentelle Vorhaben	50%	50%	40%

7.2 Status quo: Aktuelle Förderinitiativen in Deutschland

Für die deutsche IT-Sicherheitsbranche gibt es eine Vielzahl von Förderinitiativen auf EU-, Bundes- und Länderebene sowie eine Reihe von Programmen, die von der Wirtschaft in Eigeninitiative, häufig unter der Schirmherrschaft der Bundesregierung, ins Leben gerufen wurden. Die Initiativen und Programme verfolgen unterschiedliche Ziele, da sie bis auf wenige Ausnahmen entweder die IKT-Branche insgesamt ansprechen oder allgemein der Wirtschafts- und Exportförderung dienen. Das „Arbeitsprogramm IT-Sicherheitsforschung" der Bundesregierung, welches vom Bundesministerium für Bildung und Forschung (BMBF) gemeinsam mit dem Bundesministerium des Innern (BMI) im August 2009 gestartet wurde, ist hingegen ein ausschließlich auf die IT-Sicherheitsbranche ausgerichtetes Förderprogramm. Das Programm wird operationell unter dem Dach des weitaus umfangreicheren Programms „IKT 2020" des BMBF und des Bundesministeriums für Wirtschaft und Technologie (BMWi) durchgeführt.

Die ausgesuchten Programme werden im Folgenden wiederum nach den Zieldimensionen Sicherung kritischer Kompetenz, Innovation und Wachstum gegliedert.

Die folgende Tabelle gibt einen Überblick über die nachfolgend näher beschriebenen Initiativen und Programme.

Tabelle 15: Übersicht über die untersuchten Förderinitiativen und -programme

AUSWAHL

Ziele	Bund	Länder	EU	Wirtschaft
Sicherung	▪ IT-Sicherheitsforschungsprogramm (Zukunftsfonds) ▪ Forschung für die zivile Sicherheit ▪ Netzwerk elektronischer Geschäftsverkehr	▪ secure-it.nrw ▪ Hessen-IT ▪ Sicherheitsforum Baden-Württemberg	▪ 7. Rahmenprogramm ▪ IKT-Forschung "Vertrauen und Sicherheit" ▪ ENISA	▪ Deutschland sicher im Netz ▪ Arbeitsgemeinschaft für Sicherheit in der Wirtschaft (ASW) ▪ Verband für Sicherheit in der Wirtschaft (VSW) NRW e. V.
Innovation	▪ IKT 2020		▪ 7. Rahmenprogramm ▪ CIP	▪ Das Bayerische IT-Sicherheitscluster
Wachstum	▪ Arbeitsprogramm IT-Sicherheitsforschung ▪ IT-Investitionsprogramm ▪ Förderung der IKT ▪ Nationale Kontakstelle Sicherheitsforschung (NKS) ▪ Auslandsmessebeteiligungen ▪ Exportkredite (Hermes-Bürgschaften) ▪ GTAI	▪ Hessen-IT	▪ Competitiveness and Innovation Framework Programme (CIP)	▪ ITSMIG ▪ Auslandshandelskammern (AHK)

7.2.1 Beurteilung im Hinblick auf die herausgestellten Handlungsfelder

Die Förderlandschaft für IT-Sicherheit in Deutschland ist sehr vielfältig. Neben der Bundesregierung (in der die Zuständigkeiten auf mehrere Ressorts verteilt sind, insbesondere BMI, BMWi und BMBF) betätigen sich auch die Bundesländer auf diesem Gebiet. Die Wirtschaft hat ebenfalls diverse Initiativen und Institutionen ins Leben gerufen, die sich im Wesentlichen mit der Bereitstellung von Informationen für Unternehmen befassen. Hinzu kommt das milliardenschwere Forschungsprogramm der EU.

Für die Unternehmen ist es nicht leicht, sich einen Überblick über die möglichen Förderprogramme zu verschaffen. Auch in dieser Studie kann nur eine Auswahl von Programmen dargestellt werden. Es gibt zwar eine Reihe von Informationsportalen zu verschiedenen Programmen, die aber oft (wie z. B. im Fall der Nationalen Kontaktstelle für das 7. EU-Rahmenprogramm beim BMBF) mit einer sehr bürokratisch anmutenden Informationsfülle keine im Hinblick auf die Informationsbedürfnisse von KMU aufbereitete praktische Hilfe bieten. Wenn es politisch gewollt ist, die Beteiligung der KMU innerhalb der deutschen IT-Sicherheitsbranche (deren Anteil ja sehr hoch ist) an FuE-Programmen zu erhöhen, ist also eine besondere Anstrengung in diesem Bereich notwendig, insbesondere im Sinne eines Abbaus von Bürokratie.[120] Es fehlt an einer zentralen Anlaufstelle in Deutschland, die alles in einem „One-stop-Shop" bündelt, die Informationen für Unternehmen strukturiert und verständlich aufbereitet und gezielte Beratung und Hilfe bei der Bewältigung der Antragstellung bietet.

Was die Zusammenarbeit der verschiedenen Regierungsstellen im Hinblick auf die Förderung der IT-Sicherheit in Deutschland angeht, so sind mit dem „Arbeitsprogramm IT-Sicherheitsforschung" erstmals Ansätze einer sicherheitsspezifischen Grundlagenförderung erkennbar. Ähnlich der „High-Tech"-Strategie der Bundesregierung könnte in Ergänzung hierzu eine ressortübergreifende Informations-Strategie für die Förderung der IT-Sicherheitsbranche erstellt werden, die die unterschiedlichen Anforderungen auf Nachfragerseite bündelt und einen Informationsrahmen für die aktuellen und künftigen Akti-

[120] Booz & Company, Analyse der bestehenden Informationsportale

vitäten der Bundesregierung – von der Forschung bis zur Exportunterstützung – bereithält.

Eine gesamtheitliche Branchenförderung sollte jedoch von der Forschungsbis zur Exportförderung das gesamte Spektrum der Wertschöpfungskette überblicken und z. B. durch Clusterbildung und Exzellenzförderung die Wirkungskraft der Branche erhöhen. Eine Konzentration allein auf die Forschungsprogramme wäre insofern problematisch, als diese mit dem EU-Beihilferecht im Einklang stehen müssen. Damit ginge der Bundesregierung also Spielraum verloren, im Bereich der IT-Sicherheitsforschung wichtige Akzente zu setzen.

Wie in den Interviews geäußert wurde, fehlt es momentan an sogenannter hochriskanter Forschung, d. h. Forschung mit höchst ungewissem Ausgang. Diese Art der Forschung ist für den Bereich der IT-Sicherheit von besonderer Bedeutung, insofern es darum geht, im Verfahren von „trial and error" (ähnlich wie auf Angreiferseite) neue Abwehrmöglichkeiten gegen künftige Bedrohungen zu erproben. Diese Art der Forschung zählt nicht zur Grundlagenforschung, sondern eher zur experimentellen Entwicklung und kann daher von staatlicher Seite nur mit maximal 60% bei kleinen Unternehmen bzw. 50% bei mittleren Unternehmen gefördert werden. Andererseits sind die Unternehmen jedoch oft nicht bereit, die verbleibenden 50% mit eigenem Risikokapital abzudecken, da das unternehmerische Risiko in diesem Bereich zu hoch ist. Hinzu kommt, dass der ohnehin wenig entwickelte Wagniskapitalmarkt in Deutschland seit der Schließung des „Neuen Markts" wenig Alternativen für die Finanzierung von risikobehafteten Projekten bietet.

Es muss daher im Interesse des Staates liegen, die experimentelle Hochrisikoforschung und -entwicklung zu fördern, d. h. die hierfür notwendigen Förderinstrumente zu schaffen und die entsprechenden finanziellen Mittel bereitzustellen. Deutschland sollte daher einen Schwerpunkt auf die nachhaltige Entwicklung des Wagniskapitalmarkts setzen, etwa nach dem Beispiel Israels (vgl. den Ländervergleich in Abschnitt 7.4): Dort wurde er zunächst mit staatlichen Mitteln gefördert und ist nun mit über 12 Mrd. US-Dollar zum zweitgrößten Wagniskapitalmarkt der Welt (nach den USA) aufgestiegen.

7.2.2 Initiativen auf Bundesebene

Die Bundesregierung hat 2006 ein 6-Milliarden-Euro-Programm zur Förderung von Forschungs- und Entwicklungsvorhaben (FuE) verabschiedet. Mit

diesem Programm soll der Anteil von Aufwendungen für Forschung und Entwicklung am Bruttoinlandsprodukt bis 2010 auf die in der Lissabon-Strategie der Europäischen Union vereinbarten drei Prozent gesteigert werden.

Zwei Schwerpunkte im 6-Milliarden-Euro-Programm zielen direkt auf die IT-Sicherheitsbranche. Zum einen stärkt das Programm die Forschung in Informations- und Kommunikationstechnologie, und zum anderen fördert das Programm gezielt Vorhaben in den folgenden Bereich der IT-Sicherheit:

- Früherkennung und Bekämpfung von trojanischen Pferden und Viren,
- vertrauenswürdige Hard- und Softwareplattformen,
- sichere Gesamtlösungen für mobile Kommunikationsgeräte,
- Entwicklung des digitalen Personalausweises zur sicheren und eindeutigen elektronischen Identifizierung sowie eines verbindlichen und rechtssicheren Kommunikationsraums im Internet inklusive erster Pilotanwendungen im Rahmen der E-Government-Politik der Bundesregierung.

Mit dem 6-Milliarden-Euro-Programm hat sich die Bundesregierung auch gezielt dem Mittelstand gewidmet. Die Innovationsbeteiligung kleiner und mittlerer Unternehmen wird dabei weiter erhöht, die Innovationsfinanzierung verbessert und die Verwertung von Forschungsergebnissen intensiviert.

Ebenso Teil des Programms ist die Exzellenzinitiative von Bund und Ländern, die es ausgewählten Universitäten ermöglicht, sich zu international sichtbaren Spitzenzentren der Forschung mit einem eigenen Profil zu entwickeln.

Diese Exzellenzförderung ist eingebettet in die allgemeine Forschungsförderung der Bundesregierung an den über 394 Hochschulen (davon 104 Universitäten und 189 Fachhochschulen). Mit dem Programm „ProfilNT“ wird beispielsweise eine höhere Beteiligung der Fachhochschulen an Fachprogrammen des BMBF (wie z. B. Sicherheitsforschung, Mikrosystemtechnik, IKT) nachhaltig unterstützt.[121]

Die im Folgenden vorgestellten Fördervorhaben der Bundesressorts BMBF, BMWi und BMI aus dem Bereich der IT-Sicherheit werden überwiegend aus Mitteln dieses Programms finanziert. Neben der reinen FuE-Förderung betreibt die Bundesregierung Unterstützungsprogramme von der Exportunter-

[121] Bekanntmachung des BMBF vom 2. Februar 2007

stützung (z. B. Gemeinschaftsstände bei ausländischen Messen oder Hermes-Bürgschaften) über Informationsportale bis hin zu Beratungsstellen zu Forschungsprogrammen und Antragsverfahren. Die folgende Tabelle gibt einen nach den Zieldimensionen Sicherung, Innovation und Wachstum geordneten Überblick über die in dieser Studie näher betrachteten Programme auf Bundesebene mit kurzer Darstellung des Schwerpunkts und, soweit bekannt, des Fördervolumens.

Tabelle 16: Übersicht über die Förderprogramme und Initiativen des Bundes

AUSWAHL

Ziele	Name des Programms	Träger	Schwerpunkt	Volumen (Euro)
Sicherung	▪ IT-Sicherheitsforschungs-programm (Zukunftsfonds)	▪ BSI, BMI	▪ Anwendungsbezogene Innovationen ▪ Internet-Frühwarnsysteme, Trusted Computing, Biometrie und Ausweissysteme	▪ 36,5 Mio.
	▪ Forschung für die zivile Sicherheit	▪ BMBF	▪ Szenarienorientierte Sicherheitsforschung und Technologieverbünde	▪ 123 Mio.
	▪ Netzwerk elektronischer Geschäftsverkehr	▪ BMWi	▪ Informationsportal	▪ ~ 1 Mio.
Innovation	▪ IKT 2020	▪ BMBF, BMWi	▪ IKT-Wirtschaft, Automobil, Maschinenbau, Medizin, Logistik und Energie. ▪ Qualitätsziele: Wirtschaftlichkeit, **Sicherheit,** Nutzerfreundlichkeit und Ressourceneffizienz	▪ 1,5 Mrd.
Wachstum	▪ Arbeitsprogramm IT-Sicherheitsforschung	▪ BMBF, BMI	▪ Industrielle Forschungs- und experimentelle Entwicklungsvorhaben zu "Sicherheit in unsicherer Umgebung", "Schutz von Internet-Infrastrukturen", "Eingebaute Sicherheit", "Neue Herausforderungen" ▪ Deutsche Unternehmen; vor allem KMU	▪ 30 Mio.
	▪ IT Investitionsprogramm	▪ BMI	▪ Teil des Konjunkturpakets II ▪ IT-Sicherheit (ITS) ein Schwerpunkt: u.a. Krypto-Handys, Netze	▪ 202 Mio. für ITS
	▪ Förderung der IKT	▪ BMWi	▪ Anwendungsorientierte Forschungs- und Demonstrationsprojekte zu „Internet der Dinge" und „Mobiles Internet", z.B. SimoBIT - Sichere Anwendung der mobilen Informationstechnik in Mittelstand und Verwaltung	▪ 60 Mio. für SimoBIT
	▪ Nationale Kontaktstelle Sicherheitsforschung (NKS)	▪ BMWi	▪ Beratung über Forschungsprgramme	
	▪ Auslandsmesse-beteiligungen	▪ BMWi, BAFA	▪ Exportunterstützung ▪ Gemeinschaftstände bei ausländischen Messen ▪ Messeprogramm junge innovative Unternehmen	▪ 37 Mio. ▪ 3 Mio.
	▪ Exportkredit (Hermes-Bürgschaften)	▪ BMWi	▪ Förderung der Exportfinanzierung	
	▪ GTAI	▪ BMWi ▪ BMVBS	▪ Informationsportal für Außenwirtschaftsinformationen	

„Wachstum"

Arbeitsprogramm IT-Sicherheitsforschung (BMBF, BMI)

Das Arbeitsprogramm IT-Sicherheitsforschung ist die jüngste und gezielteste Förderungsinitiative zum Thema IT-Sicherheit. Die Ziele des Programms umfassen

- die Schaffung der Grundlagen für die Entwicklung überprüfbar und durchgehend sicherer IT-Systeme,
- die Erforschung neuer Ansätze bei der Analyse und Absicherung von IKT-Systemen,

- positive Effekte für die Wettbewerbsfähigkeit des Forschungs-, Produktions- und Arbeitsplatzstandortes Deutschland im Bereich IT-Sicherheit sowie
- die Verwertbarkeit von Forschungsergebnissen auch außerhalb des sicherheitsrelevanten Bereichs, sofern dies die Sicherheitsinteressen Deutschlands zulassen.

Ein Schwerpunkt der ersten Förderrunde ist das Thema „Sicherheit in unsicheren Umgebungen".

Weitere Schwerpunkte umfassen:

- Schutz von Internet-Infrastrukturen,
- eingebaute Sicherheit,
- neue Herausforderungen beim Schutz von IT-Systemen und der Identifikation von Schwachstellen.[122]

Das „Arbeitsprogramm IT-Sicherheitsforschung" wurde am 3. September 2009 veröffentlicht, hat eine Laufzeit von fünf Jahren und ist vom BMBF mit Fördermitteln in Höhe von 30 Mio. Euro ausgestattet. Die operative Umsetzung des Programms wird im Rahmen des BMBF-Programms „IKT 2020 – Forschung für Innovationen" erfolgen.[123]

Das Programm wendet sich sowohl an Unternehmen (insbesondere KMU) mit Sitz und überwiegender Ergebnisverwertung in Deutschland als auch an Hochschulen, Forschungseinrichtungen und andere FuE-Institutionen sowie Behörden. Diese Fördermaßnahme unterstützt industrielle Forschungs- und experimentelle Entwicklungsvorhaben zur Stärkung der Innovationsfähigkeit der Unternehmen in Deutschland.

IT-Investitionsprogramm (BMI)

Das IT-Investitionsprogramm im Rahmen des „Gesetzes für Beschäftigung und Stabilität in Deutschland (Konjunkturpaket II)" stellt in den Jahren 2009 und 2010 zusätzliche 500 Mio. Euro für die Modernisierung der Informations- und Kommunikationstechnik in der Verwaltung bereit. Für den Bereich der IT-Sicherheit sind ressortübergreifende Maßnahmen mit einem Gesamtvolu-

[122] Eckpunktepapier des BMBF und des BMI vom 3. März 2009

[123] Richtlinien zur Förderung der IT-Sicherheit, Bekanntmachung des BMBF vom 26.8.2009

men von 163 Mio. Euro und zusätzlich ressortspezifische Maßnahmen mit einem Gesamtvolumen von 39 Mio. Euro geplant, die zweifellos positive Auswirkungen auf die Nachfrage nach IT-Sicherheit in Deutschland haben. Unter anderem sollen Beratungsdienstleistungen und einheitliche, vom BSI geprüfte IT-Sicherheitsprodukte für die Bundesverwaltung beschafft werden.[124] Allerdings gibt es kritische Stimmen aus der Wirtschaft, dass die Gelder überwiegend über bestehende Rahmenverträge ausgegeben würden und somit nur Teile der deutschen IT-Sicherheitsbranche von diesem Konjunkturprogramm profitierten.[125]

Förderung der IKT (BMWi)

Dieses Förderprogramm zielt auf anwendungsorientierte Forschungs- und Demonstrationsprojekte zur Stärkung der Nutzung und Verbreitung dieser Querschnittstechnologie in Wirtschaft und Gesellschaft. Der Schwerpunkt der Förderung liegt auf der Konvergenz und dem Wissensmanagement. Im Mittelpunkt dieser Förderlinie steht das strategische FuE-Vorhaben THESEUS zur Erforschung semantischer Technologien, die Inhalte (Wörter, Bilder, Töne) nicht mithilfe herkömmlicher Verfahren (z. B. Buchstabenkombinationen) ermitteln, sondern die inhaltliche Bedeutung der Informationen erkennen und einordnen können. Im Hinblick auf die IT-Sicherheit befasst sich THESEUS unter anderen mit dem Thema Digital Rights Management zum Schutz des geistigen Eigentums.

Das Programm hat eine Laufzeit von fünf Jahren und ist mit insgesamt rund 200 Mio. Euro ausgestattet, von denen die Bundesregierung durch das BMWi ca. 100 Mio. Euro beisteuert. Die übrigen 100 Mio. Euro kommen als Eigenmittel von den beteiligten Partnern aus Industrie und Forschung. Bislang haben sich 30 Forschungseinrichtungen, Universitäten und Unternehmen mit Projektvorhaben in das THESEUS-Programm eingebracht.

Nationale Kontaktstelle Sicherheitsforschung (NKS) (BMBF)

---

[124] Übersicht über ressortspezifische und ressortübergreifende Maßnahmen des IT-Investitionsprogramms, Mitteilung des IT-Beauftragten der Bundesregierung vom 20. Juli 2009

[125] Interview mit einem deutschen IT-Sicherheitsanbieter

Die Nationale Kontaktstelle Sicherheitsforschung (NKS) bei der VDI Technologiezentrum GmbH informiert und berät Forschungseinrichtungen, Hochschulen, Universitäten und Unternehmen im Auftrag des Bundesministeriums für Bildung und Forschung kostenlos über die Möglichkeiten einer EU-Förderung im Bereich Sicherheitsforschung. Die Beratung umfasst Informationen über bestehende Förderprogramme sowie das Antragsverfahren.[126]

Messebeteiligungen (BMWi, BAFA)

Seit Juni 2007 wird die Teilnahme junger innovativer Unternehmen an Gemeinschaftsständen auf internationalen Leitmessen in Deutschland gefördert. Ziel des Programms ist es vor allem, den Export neuer Produkte und Verfahren zu unterstützen. Die exportorientierten deutschen Leitmessen bieten eine hervorragende Plattform für die Erschließung internationaler Märkte und damit für das Wachstum junger innovativer Unternehmen in Deutschland. 2008 hat das BAFA die Teilnahme von 420 jungen innovativen Unternehmen auf 36 Messeveranstaltungen gefördert. Das Programm soll bis mindestens 2013 fortgeführt und mit jährlich 3 Mio. Euro unterstützt werden. Darüber hinaus organisiert das BMWi in enger Zusammenarbeit mit dem Ausstellungs- und Messeausschuss der Deutschen Wirtschaft e. V. (AUMA) und dem BAFA regelmäßig Beteiligungen des Bundes an Messen und Ausstellungen im Ausland im Rahmen von Firmengemeinschaftsständen, an denen hauptsächlich kleine und mittlere Unternehmen teilnehmen.[127] Im Bereich der IT-Sicherheit wird die Teilnahme an der Leitmesse für IT-Sicherheit „RSA Conference“ durch einen Gemeinschaftsstand unterstützt.

Hermes-Bürgschaften (BMWi, BMF, BMZ, AA)

Die Hermes-Bürgschaften dienen insbesondere zur Erschließung von Märkten durch (auch mittelständische) deutsche Unternehmen. Im Rahmen der Hermes-Bürgschaften hat der Bund im Jahr 2008 die Gewährleistung für Auftragswerte in Höhe von 20,7 Mrd. Euro übernommen – dies entspricht rund 2,1% des deutschen Gesamtexports. Rund 90% der übernommenen Deckungen entfielen dabei auf Exporte in Entwicklungsländer bzw. in Staaten Mittel-

[126] Infoflyer des BMBF zur Nationalen Kontaktstelle Sicherheitsforschung, 2008

[127] Jahresbericht 2008, Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA), Januar 2009

und Osteuropas einschließlich der GUS-Länder.[128] Die Bürgschaften werden überwiegend von KMU genutzt.[129]

Germany Trade and Invest (GTaI) (BMWi, BMVBS)

Die Germany Trade and Invest ist die Wirtschaftsförderungsgesellschaft der Bundesrepublik Deutschland. Die GTaI ist am 1. Januar 2009 durch Zusammenführung der Bundesagentur für Außenwirtschaft und der Invest in Germany GmbH entstanden und wird vom BMWi und dem BMVBS gefördert. Sie unterstützt deutsche Unternehmen, die ausländische Märkte erschließen wollen, mit aktuellen und ausführlichen Marktanalysen, Wirtschaftsdaten und Informationen aus rund 120 Ländern. Dabei werden jedoch keine spezifischen Informationen zum IT-Sicherheitsmarkt und zu den Absatzchancen im Ausland bereitgehalten.[130]

„Innovation"

IKT 2020 – Forschung für Innovation (BMBF, BMWi)

Die Forschungsförderung des BMBF und des BMWi ist ausgerichtet auf in Deutschland starke Anwendungsfelder und Branchen, in denen die Innovationen in hohem Maße IKT-getrieben sind. Neben der IKT-Wirtschaft selbst sind dies die Branchen Automobil, Maschinenbau, Medizin, Logistik und Energie. Dabei erfolgt eine Fokussierung auf die Qualitätsziele Wirtschaftlichkeit, Sicherheit, Nutzerfreundlichkeit und Ressourceneffizienz.

Das Programm IKT 2020 setzt auf Innovationsallianzen und Technologieverbünde, die die für die IT-Sicherheit wichtige Zusammenarbeit zwischen Technologieentwicklung und Anwendung fördern. Die Förderung kleiner und mittlerer Unternehmen erfolgt dabei durch vereinfachte Förderverfahren, die Einrichtung einer zentralen Anlaufstelle sowie die Verkürzung der Zeit zwischen der Antragstellung und der abschließender Förderentscheidung

[128] Jahresbericht 2008 zu Exportkreditgarantien der Bundesrepublik, Juni 2009

[129] „Wettbewerbsbedingungen deutscher Unternehmen in den arabischen Staaten", Studie des BMWi, März 2009

[130] http://www.gtai.de/DE/Navigation/Ueber-uns/Profil/profil-node.html

bzw. der Bereitstellung der Mittel.[131] Diese Ausrichtung auf KMU ist ein notwendiger Beitrag, den von befragten Unternehmen beklagten administrativen Aufwand bei der Teilnahme an Förderprogrammen zu verringern.

„Sicherung"

IT-Sicherheitsforschungsprogramm (Zukunftsfonds) (BSI)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) behandelt in seinem eigenen IT-Sicherheitsforschungsprogramm (Zukunftsfonds), das im Rahmen des 6-Milliarden-Euro-Programms der Bundesregierung mit 36,5 Mio. Euro finanziert wird, prioritäre Fragestellungen auf dem Gebiet der IT-Sicherheit. Das Programm zielt auf anwendungsbezogene Innovationen ab, mit Schwerpunkt auf den Technologiefeldern Internet-Frühwarnsysteme, Trusted Computing, Biometrie und Ausweissysteme. Das BSI setzt dabei auf eine enge Kooperation und Verzahnung der Behörde mit den Auftragnehmern aus Forschung und Wirtschaft.[132]

„Forschung für die zivile Sicherheit – Programm der Bundesregierung" (BMBF)

Dieses vom BMBF geförderte Programm umfasst mit „Szenarienorientierte Sicherheitsforschung" und „Technologieverbünde" zwei Programmlinien, die mittelbar Themen der IT-Sicherheitsforschung bzw. -förderung einschließen. Für eine erste Förderperiode stellt das BMBF bis zum Jahr 2010 Haushaltsmittel im Umfang von rund 123 Mio. Euro bereit. Über 44 Verbundprojekte mit einem Volumen von 85,8 Mio. Euro wurden bereits gefördert.[133]

Netzwerk elektronischer Geschäftsverkehr (BMWi)

Das Netzwerk Elektronischer Geschäftsverkehr (NEG) wurde 1998 vom Bundesministerium für Wirtschaft und Technologie gegründet und berät seither in seinen derzeit 25 regionalen Kompetenzzentren sowie im Branchenzentrum Handel den Mittelstand zu allen Fragen des elektronischen Geschäfts-

[131] „IKT 2020 Forschung für Innovationen", High-Tech Strategie der Bundesregierung, BMBF, 2007

[132] Die Lage der IT-Sicherheit in Deutschland 2009, BSI, Januar 2009

[133] Informationen über abgelaufene Bekanntmachungen des BMBF

verkehrs. Die Zentren sind meist bei den Industrie- und Handelskammern und den Handwerkskammern sowie bei Technologietransferstellen und Forschungseinrichtungen angesiedelt. Der Schwerpunkt ihrer Arbeit liegt (neben der Beratung) in der Durchführung von Studien und Veranstaltungen sowie der Bereitstellung von Info-Materialien zum Thema E-Business in einem umfangreichen Informationsportal. Zielgruppe des Netzwerks sind vornehmlich Kleinunternehmer, Mittelständler und Handwerker. 70 Prozent der Betriebe, die bislang vom NEG beraten wurden, sind Kleinstunternehmen mit weniger als zehn Beschäftigten.[134]

Im Hinblick auf die IT-Sicherheit engagiert sich das Netzwerk insbesondere bei der Förderung des Sicherheitsbewussteins. In den vergangenen Jahren wurden abwechselnd aktuelle Themen schwerpunktmäßig behandelt, u. a. die IT-Sicherheit und die Radio Frequency Identification (RFID). Den Informationsbedarf im Mittelstand erfragt das NEG regelmäßig über onlinegestützte Studien. Das NEG ist darüber hinaus auf verschiedenen Messen (wie der Internationalen Handwerksmesse, der SYSTEMS und der CeBIT) vertreten.

7.2.3 Initiativen auf Landesebene

Auch auf Landesebene existieren ebenfalls eine Reihe von Initiativen, die im Folgenden nur zusammenfassend dargestellt werden.

Hessen: Hessen-IT

Hessen-IT ist ein vom Hessischen Ministerium für Wirtschaft, Verkehr und Landesentwicklung gefördertes Programm für den Informations- und Telekommunikationsmarkt in Hessen, speziell für kleine und mittlere Unternehmen. Hessen-IT bietet Beratung in Sachen IT-Sicherheit sowie eine Datenbank mit Informationen über IT-Sicherheitsanbieter und Fachthemen wie „IT-Sicherheit für den Mittelstand".[135]

---

[134] 10 Jahre Netzwerk elektronischer Geschäftsverkehr, Pressemitteilung des BMWi vom 17.12.2007

[135] http://www.hessen-it.de/dynasite.cfm?dssid=55&dsmid=734

NRW: secure-it.nrw

Die vom Land Nordrhein-Westfalen geförderte Initiative »secure-it.nrw« befasst sich seit 2001 mit IT-Sicherheit und Datenschutz. Mit den Programmen „IT-Sicherheitstag NRW", dem „IT-Sicherheitspreis NRW", der „Basisprüfung IT-Sicherheit" und dem Online-Portal www.branchenbuch-it-sicherheit.de sensibilisiert und informiert »secure-it.nrw« mittelständische Unternehmen und private Anwender. Die Förderung von »secure-it.nrw« durch das Land Nordrhein-Westfalen endete 2009. Eine Neuausrichtung mit anderer Finanzierung wird aktuell diskutiert.[136]

Baden-Württemberg: Sicherheitsforum Baden-Württemberg

Das Sicherheitsforum Baden-Württemberg ist ein vom Innenministerium des Landes Baden-Württemberg unterstütztes unabhängiges Gremium aus Firmen, Forschungseinrichtungen, Verbänden, Kammern und Behörden, das sich vornehmlich mit dem Schutz vor Wirtschaftsspionage befasst.[137]

7.2.4 Initiativen der EU

Die Europäische Union befasst sich sehr intensiv mit den Fragen der IT-Sicherheit. Neben der Generaldirektion „Informationsgesellschaft und Medien" hat die EU die Europäische Agentur für Netz- und Informationssicherheit (ENISA) ins Leben gerufen. Hinzu kommt erstmalig die Sicherheitsforschung als Teil der umfangreichen Forschungsrahmenprogramme.

„Sicherung"

IKT-Forschung „Vertrauen und Sicherheit"

Die Europäische Kommission unterhält in der Generaldirektion Informationsgesellschaft und Medien eine Abteilung für „Trust and Security", deren vorrangige Aufgabe darin besteht, die Forschung mit dem Ziel der Entwicklung vertrauenswürdiger IKT zu unterstützen und zu koordinieren.

---

[136] Info-Flyer zur Landesinitiative „secure-it.nrw" für mehr Datensicherheit, Oktober 2007

[137] http://www.sicherheitsforum-bw.de/ueber_uns/index.htm

Die Forschungsschwerpunkte liegen in der Entwicklung des Internets der Zukunft: vertrauenswürdige Netzwerk- und Dienste-Infrastruktur, Identitätsmanagement, sichere Software, Trusted Computing, Kryptographie und fortgeschrittene Biometrie. Zur Erreichung der Ziele wurden drei Arbeitsbereiche definiert:

- **Forschungsförderung** über Rahmenprogramme (z. B. 7. Rahmenprogramm),
- **Anreize für die Annahme von vertrauenswürdiger und sicherer IKT** durch das Wettbewerbs- und Innovationsprogramm „IKT Unterstützungsprogramm (CIP ICT-PSP)“,
- **Weiterentwicklung der Forschungspolitik**.

Europäische Agentur für Netz- und Informationssicherheit (ENISA)

Die Europäische Union hat ferner die Europäische Agentur für Netz- und Informationssicherheit (ENISA) als zentrale Anlauf- und Beratungsstelle für die Mitgliedstaaten und die EU-Organe in Fragen der Netz- und Informationssicherheit eingerichtet. Sie hat im September 2005 ihre Arbeit aufgenommen. Die ENISA unterstützt die Mitgliedstaaten, die EU-Organe und die Wirtschaft bei der Bewältigung der Probleme im Bereich der Netz- und Informationssicherheit.

Die Tätigkeitsschwerpunkte der ENISA sind:

- Beratung und Unterstützung der Kommission und der Mitgliedstaaten in ihrem Dialog mit der Industrie, um sicherheitsrelevante Probleme bei Hardware- und Softwareprodukten anzugehen,
- Erhebung von Informationen zur Analyse der derzeitigen und absehbaren Risiken in Europa,
- Förderung von Risikobewertungs- und Risikobewältigungsverfahren zur Verbesserung der Fähigkeit, mit Gefahren für die Informationssicherheit umzugehen,
- Austausch bewährter Verfahren zur Sensibilisierung und Zusammenarbeit zwischen den verschiedenen Akteuren im Bereich der Informationssicherheit, insbesondere durch die Entwicklung einschlägiger öffentlich-privater Partnerschaften mit der Industrie,

- Begleitung der Entwicklung von Standards für Produkte und Dienstleistungen im Bereich der Netz- und Informationssicherheit.

„Innovation"

7. Rahmenprogramm, EU

Bis 2013 stellt die EU mehr als 50 Mrd. Euro für das 7. Forschungsrahmenprogramm zur Verfügung. Für die Forschungsförderung im Themenbereich „Sicherheit" werden im Zeitraum von 2007 bis 2013 insgesamt 1,4 Mrd. Euro bereitgestellt. Das BMBF unterhält unter www.forschungsrahmenprogramm.de ein zentrales Informationsportal, auf dem Informationen über Programme und Antragsverfahren bereitgehalten werden. Die Beteiligung an den Ausschreibungen zu diesem Programm ist jedoch mit hohem administrativen Aufwand verbunden, nicht zuletzt wegen des sehr umfangreichen Informationsmaterials. Diese administrative Hürde ist daher für Hochschulen und Forschungseinrichtungen erheblich leichter zu überwinden als für KMU. Beim Vorgängerprogramm, dem 6. EU-Rahmenprogramm, sind über 3 Mrd. Euro (18 Prozent des gesamten EU-Fördervolumens und damit der größte „Topf" an EU-Fördermitteln) an deutsche Forschungseinrichtungen geflossen.[138] Angaben zum aktuellen Programm liegen noch nicht vor.

„Wachstum"

Competitiveness and Innovation Framework Programme (CIP), EU

Das CIP zielt auf die Verbesserung der Wettbewerbsfähigkeit europäischer Unternehmen. Dabei liegt der Schwerpunkt der Förderung auf kleinen und mittleren Unternehmen. Thematisch unterstützt dieses Programm innovative Aktivitäten durch den verbesserten Zugang zu Finanzmitteln und stellt Dienstleistungen für die Unterstützung von Geschäftstätigkeiten in den Regionen zur Verfügung. Das CIP-Programm fördert auch die Verfügbarkeit und Nutzung von IKT. Das Programm hat eine Laufzeit von sieben Jahren (2007–2013) und einen finanziellen Rahmen von 3,621 Mrd. Euro.

[138] Förderranking 2009, Deutsche Forschungsgemeinschaft, September 2009

7.2.5 Initiativen der deutschen Wirtschaft

In der vorliegenden Studie werden neben einer Auswahl staatlicher Programme auch eine Reihe von Initiativen und Plattformen der Wirtschaft untersucht, die mittelbar und unmittelbar die Unternehmen der IT-Sicherheitsbranche in Deutschland in ihren Aktivitäten unterstützen.

„Sicherung"

Deutschland sicher im Netz, BMI (Schirmherrschaft)

Der Verein „Deutschland sicher im Netz" hat das Ziel, bei den Verbrauchern und in den Unternehmen ein Bewusstsein für einen sicheren Umgang mit Internet und IT zu fördern. Der Kooperationsvertrag mit dem Bundesministerium des Innern (BMI) hat die Rolle von DsiN e. V. weiter bestärkt. Des Weiteren ist das BSI Beiratsmitglied von DsiN und unterstützt aktiv die Arbeit des Vereins. Mit konkreten Aktionen und Services bietet DsiN Verbrauchern, besonders auch Kindern und Jugendlichen, sowie kleinen und mittelständischen Unternehmen Hilfestellung und praktische Lösungen rund um die IT-Sicherheit an und fördert dadurch das Sicherheitsbewusstsein der Bürger und der Wirtschaft

Die im Jahr 2006 durch die Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) ins Leben gerufene Kampagne „Online kaufen – mit Verstand" wurde mittlerweile als Bestandteil in die Aktivitäten von „Deutschland sicher im Netz e. V." eingebunden.

Arbeitsgemeinschaft für Sicherheit in der Wirtschaft (ASW)

Zweck der ASW ist es, die Sicherheitsbelange der gewerblichen Wirtschaft gegenüber Regierung, Politik und Verwaltung zu vertreten. Die ASW ist ein Zusammenschluss der Spitzenorganisationen der deutschen Wirtschaft, aller deutschen regionalen Sicherheitsverbände (VSWn) sowie mehrerer Branchenverbände in Sicherheitsfragen. Die ASW ist damit die Zentralorganisation der deutschen Wirtschaft in Sicherheitsfragen. Derzeit wird die Arbeit der ASW von 17 Mitgliedsorganisationen unterstützt.[139]

[139] http://www.asw-online.de/verband/index.php

NRW: Verband für Sicherheit in der Wirtschaft (VSW) NRW e. V.

Der Verband für Sicherheit in der Wirtschaft (VSW) ist ein Wirtschaftsverband, der den Stellenwert von Sicherheit im Unternehmen fördert und auch Mitglied im ASW ist. Der VSW hat 165 Mitgliedsunternehmen aus Großindustrie und Mittelstand und bietet im Dialog mit Wirtschaft, Politik und Behörden qualifizierte Leistungen wie Publikationen, Seminare und Veranstaltungen rund um das Thema Sicherheit im Unternehmen an. Herauszuheben ist dabei die „Sicherheitspartnerschaft NRW", bei der der VSW im Oktober 2001 zur Förderung der Belange des Wirtschafts- und Geheimschutzes gemeinsam mit der Vereinigung der Industrie- und Handelskammern in Nordrhein-Westfalen eine Public-Private-Partnership mit dem Innen- und Wirtschaftsministerium NRW vereinbart hat. Wesentlicher Gegenstand dieser Partnerschaft ist die Intensivierung der Zusammenarbeit von Staat und Wirtschaft bei der Bekämpfung von Wirtschaftsspionage und Wirtschaftskriminalität.[140]

„Innovation"

Das Bayerische IT-Sicherheitscluster

Das Bayerische IT-Sicherheitscluster wurde 2006 gegründet und besteht aus 43 Unternehmen und vier Hochschulen. Seine Ziele sind insbesondere die Förderung der Forschung und Qualifizierung im Bereich der IT-Sicherheit sowie die Bereitstellung von Informationen über Sicherheitsrisiken und technische Lösungen. Die Kooperation der Aktivitäten namhafter Universitäten in der IT-Sicherheitsforschung und -entwicklung und die Ausgründung von Unternehmen in diesem Cluster wird vom Land Bayern gezielt unterstützt. So fördert das Wirtschaftsministerium des Landes Bayern derzeit ein Projekt zur Entwicklung von Lösungen für Kleinunternehmen zum Schutz des elektronischen Datenaustauschs mit 900.000 Euro. Das bayerische Wissenschaftsministerium unterstützt eine Kooperation des Clusters mit der Automobilindustrie zur Entwicklung sicherer Software für Steuergeräte in Fahrzeugen.[141]

---

[140] http://www.sicherheit-in-der-wirtschaft.de/der-vsw-nw/profil

[141] http://www.it-sicherheit-bayern.de/kompetenz/0-517,1,0.html

„Wachstum“

ITSMIG e.V.

„IT Security made in Germany (ITSMIG e.V.)“ ist ein eingetragener Verein zur Unterstützung der Exportchancen deutscher Unternehmen der IT-Sicherheitsbranche. Der Verein ist 2005 aus einer Initiative der damaligen Bundesminister Schily (BM des Innern) und Clement (BM für Wirtschaft und Arbeit) entstanden. Nach anfänglicher Anschubfinanzierung durch den Bund erfolgt die Unterstützung nunmehr in Form einer gemeinsamen Schirmherrschaft des BMWi und des BMI, die auch im Beirat des Vereins vertreten sind.

Der ITSMIG e. V. hat derzeit 24 Mitgliedsfirmen, die alle sowohl mehrheitlich in deutschem Besitz sind als auch ihre überwiegenden Forschungs- und Entwicklungsleistungen in Deutschland erbringen.

Der geographische Schwerpunkt der Exportförderung wurde durch eine Mitgliederbefragung im Jahre 2006 auf den Nahen und Mittleren Osten, Südostasien sowie Mittel- und Osteuropa festgelegt. Die Exportförderung erfolgt in Form von koordinierter Informationsbeschaffung und Marktbeobachtung. Zu diesem Zweck betreibt die ITSMIG e.V. in Abu Dhabi eine Marktbeobachtungsstelle für den gesamten Nahen und Mittleren Osten. Die ITSMIG e.V. wird bei ihren Tätigkeiten vom BMWi, dem BMI sowie der örtlichen Auslandsvertretung des AA unterstützt. Bei den im Rahmen dieser Studie durchgeführten Interviews wurde jedoch von den befragten Unternehmen der Wunsch nach einer besseren Abstimmung innerhalb der Bundesregierung (vor allem im Hinblick auf das Auswärtige Amt) geäußert. Zudem wurde die finanzielle und damit personelle Ausstattung der ITSMIG e.V. als nicht ausreichend bezeichnet, um mit den USA und Frankreich in der Exportförderung mithalten zu können.

Auslandshandelskammern (AHK)

Die AHKs sind ein wichtiger Partner im Ausland für die Außenwirtschaftsförderung durch das Bundesministerium für Wirtschaft und Technologie. Sie vertreten – zusammen mit den deutschen Auslandsvertretungen (Botschaften und Konsulate) – offiziell die Interessen der deutschen Wirtschaft gegenüber der Politik und Verwaltung im jeweiligen Gastland. Diese Funktion verpflichtet die AHKs zur Neutralität und Objektivität gegenüber den Unternehmen.

7.3 Besondere Anforderungen im Hinblick auf den Schutz von öffentlichen Interessen

Der Schutz der Sicherheitsinteressen des Staates ist für die IT-Sicherheitsbranche eine vielfältige Herausforderung. Neben der IKT als kritischer Infrastruktur gehören die konsequente Anwendung von IT-Sicherheitsstandards sowie die Bereitstellung einer „vertrauensvollen Werkbank" in diese Betrachtung.

Der nationale Plan zum Schutz der kritischen Infrastruktur stuft die IKT zur Gänze als kritische Infrastruktur ein, da sie durch die zunehmende Vernetzung vieler lebenswichtiger Systeme und Funktionen das zentrale Nervensystem darstelle. Die Sicherung der IKT-Infrastruktur erfordert daher eine konsequente Anstrengung, und damit kommt der deutschen IT-Sicherheitsbranche eine zentrale Rolle zu. Diesem Stellenwert trug bereits das Telekommunikationsgesetz von 1997 Rechnung, das die Telekommunikationsbetreiber auf bestimmte Sicherheitsanforderungen verpflichtete und zugleich die Einhaltung dieser Verpflichtungen unter staatliche Kontrolle stellte (ausgeübt durch die Bundesnetzagentur). Auch bei der Beschaffung der öffentlichen Hand ist die Sicherung der IKT durch IT-Sicherheitsstandards und Gewährleistung der Interoperabilität der **Verwaltungs**systeme sicherzustellen.

Ein großes Politikfeld, in dem die Interessen der Bundesrepublik berührt sind, ist das Außenwirtschaftsrecht. Die IT-Sicherheitsindustrie unterliegt zum einen mit einem Teil ihrer Produkte und Technologien der Exportkontrolle und zum anderen den Regelungen des § 7 AWG. Letzterer gibt der Bundesregierung die Möglichkeit, ausländische Beteiligungen an deutschen Unternehmen, die sicherheitsrelevante Kryptosysteme herstellen, einer besonderen Prüfung zu unterziehen und gegebenenfalls zu beschränken, wenn dies aus Gründen der öffentlichen Ordnung oder Sicherheit der Bundesrepublik Deutschland unerlässlich ist. Eine solche Prüfung ist z. B. im Fall der Übernahme der Utimaco AG durch die britische SOPHOS geschehen.[142] Neben dem Schutz bestehender deutscher Unternehmen muss sich der Staat auch Gedanken darüber machen, eine durchgängige Wertschöpfungskette für die Entwicklung und Herstellung von IT-Hochsicherheitstechnologie im Sinne einer „vertrauensvollen Werkbank" verfügbar zu halten. Insbesondere im

[142] „Strategische Industrie IT", Dr. Hans Bernhard Beus, griephan global security 1/2009

Hochsicherheitsbereich wurde von einigen Interviewpartnern eine Unabhängigkeit von ausländischen Herstellern und damit von ausländischen Staatsinteressen als erforderlich angesehen. In der Vergangenheit sind (wie schon erwähnt) bereits Unternehmen aus dem Bereich der Basisinfrastruktur, zum Beispiel Mobiltelefonhersteller, vom deutschen Markt verschwunden. Eine sorgfältige Beantwortung der Frage, welche Industriebereiche im Inland benötigt werden, und eine darauf aufbauende gezielte Förderung der in Deutschland fehlenden Komponenten liegt daher im Sicherheitsinteresse Deutschlands.

Das Beispiel der IT-Sicherheitsbranche in Deutschland als einer wichtigen Schlüsselindustrie zeigt auch die Bedeutung eines gut funktionierenden Kapitalmarktes für die Sicherheitsinteressen der Bundesrepublik Deutschland. Die überwiegend mittelständische Struktur der hiesigen IT-Sicherheitsindustrie und die fehlenden Finanzierungsmöglichkeiten (insbesondere über Wagniskapital für kleine und mittelständische Unternehmen im Hochtechnologiebereich) machen diese Unternehmen besonders anfällig für Übernahmen durch die internationale Konkurrenz.

7.4 Initiativen im internationalen Ländervergleich

Im internationalen Vergleich spielt die deutsche IT-Sicherheitsbranche keine herausragende Rolle. Für die Ableitung von Handlungsoptionen für die Bundesregierung ist es daher unerlässlich, die wichtigsten Märkte für die IT-Sicherheit näher zu untersuchen. Für diese Studie wurden die Länder China, Frankreich, Großbritannien, Korea, Israel und die Vereinigten Staaten zum Vergleich herangezogen. Während der Befragung haben viele Unternehmen angegeben, dass der Massenmarkt für IT-Sicherheitsprodukte von amerikanischen Unternehmen dominiert werde und für deutsche Unternehmen kaum noch zu erschließen sei. Dies sei vor allem auf die Skaleneffekte und die globale Präsenz der amerikanischen Unternehmen zurückzuführen. Allerdings haben die übrigen Länder, die im Folgenden vorgestellt werden, allen voran Israel, sehr erfolgreiche Unternehmen in der IT-Sicherheitsbranche hervorgebracht. Es scheint daher angezeigt, die wichtigsten Faktoren herauszuarbeiten, die den jeweiligen Erfolg begründen.

Vielfach hängt der Erfolg der IT-Sicherheitsindustrie mit der Stellung und Förderung des IKT-Marktes insgesamt in diesen Ländern zusammen. Da es kein anerkanntes internationales Ranking für die IT-Sicherheit gibt, bietet sich ein Blick auf die großen internationalen IKT-Rankings der Vereinten Nationen (UN), der Internationalen Telekommunikationsunion (ITU) sowie des World Economic Forum (WEF) an. Im Vergleich der Länder mit Blick auf die E-Government- und IKT-Readiness ergibt sich, dass die obersten Plätze in der Regel durch die skandinavischen sowie die ostasiatischen Länder besetzt werden. Deutschland belegt eher mittlere Plätze, was sich im Ergebnis auch auf die Situation auf dem IT-Sicherheitsmarkt sowie generell auf die Exportchancen auswirkt. Länder des Mittleren Ostens zum Beispiel nutzen die Rankings als Auswahlkriterium in dem Sinne, dass nur Firmen aus Ländern, die auf den ersten fünf Plätzen stehen, bei großen Beschaffungsvorhaben berücksichtigt werden. Auch wenn dies keine wissenschaftliche Methode ist, beeinflusst das Abschneiden eines Landes bei solchen Rankings also die Exportchancen seiner Industrie. Die Bundesrepublik sollte daher ein wirtschaftliches Interesse daran haben, diese Rankings ernst zu nehmen und möglichst gut abzuschneiden.

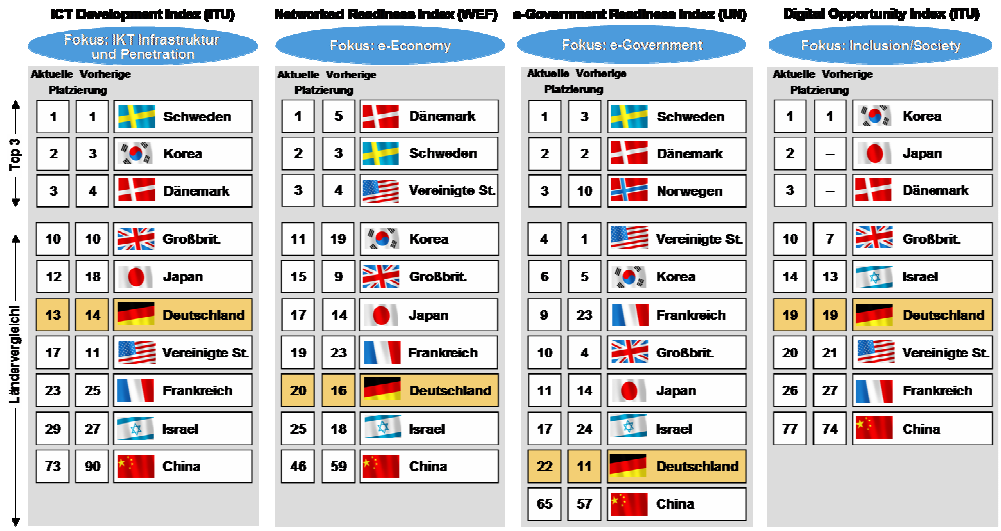


Abbildung 37: Ländervergleich internationaler Rankings[143]

Generell können die Ergebnisse in den internationalen Vergleichen mit dem Gesamtaufwand in Verbindung gebracht werden, den jedes Land für die IKT verwendet. Die führenden Nationen haben, gemessen am Bruttoinlandsprodukt, durchweg höhere anteilige IKT-Ausgaben, wie die folgende Abbildung veranschaulicht. Am Beispiel China ist sehr gut zu erkennen, wie sich die hohen IT-Ausgaben in der Verbesserung der Platzierung in den Rankings der ITU und des WEF widerspiegeln, die sich auf die Infrastruktur und die Netzverfügbarkeit konzentrieren. Im ITU Ranking konnte China eine Verbesserung von Platz 90 auf Platz 73 erzielen, beim WEF Ranking eine Verbesserung von Platz 59 auf Platz 46.

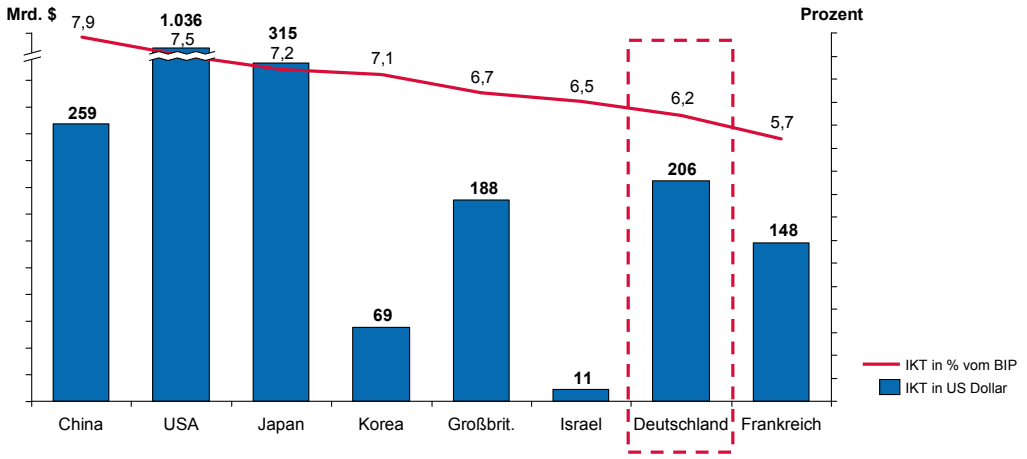


Abbildung 38: IKT-Ausgaben 2007 in Prozent des BIP (in US-Dollar)[144]

[143] ITU 2009; WEF; UN; Booz & Company Analyse

Hinzu kommt die Frage, welchen Anteil die IKT-Ausfuhren (sowohl Waren als auch Dienstleistungen) an den Gesamtausfuhren eines Landes haben. Die folgende Abbildung verdeutlicht, dass die IKT-Branche insgesamt in Deutschland für die Ausfuhr und somit für die Nachfrage im Ausland noch erheblichen Nachholbedarf hat.

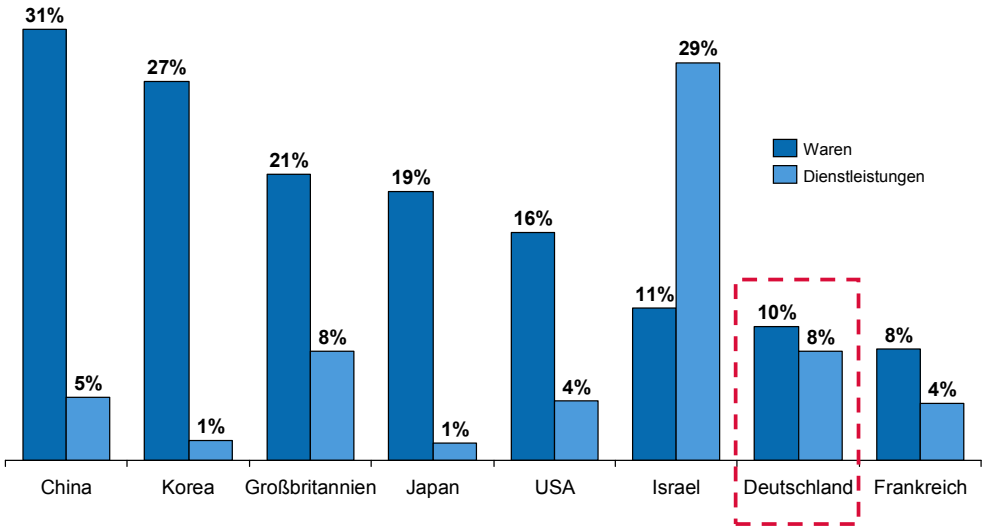


Abbildung 39: Anteil der IKT-Ausfuhren (Waren und Dienstleistungen) an der jeweiligen Gesamtausfuhr[145]

Zur Stärkung des Wirtschaftswachstums und der Wettbewerbsfähigkeit hat die Europäische Union mit der Lissabon-Strategie das Ziel verbunden, die Aufwendungen (öffentliche und private) für Forschung und Entwicklung auf 3% des europäischen BIP zu steigern. Dem liegt die Erkenntnis zugrunde, dass unter den Industrienationen im Ergebnis solche Volkswirtschaften besonders erfolgreich sind, die überdurchschnittlich in Forschung und Entwicklung investieren. Die Bundesregierung hat mit dem 6-Milliarden-Euro-Programm von 2006 die öffentlichen FuE-Ausgaben erhöht. Von rund 9 Mrd. Euro im Jahr 2005 sind die Ausgaben 2007 auf über 10,1 Mrd. Euro gestiegen. Die Länder haben ebenfalls ihre FuE-Ausgaben auf 8,3 Mrd. Euro im Jahre 2007 gesteigert. Die FuE-Aufwendungen der Wirtschaft sind im Jahr 2006 auf 41,1 Mrd. Euro gestiegen. Das nachfolgende Schaubild zeigt, wo sich Deutschland im internationalen Vergleich der FuE-Aufwendungen befindet.

---

[144] World Bank; Global Insight/WITSA, IMF, Booz & Company Analyse

[145] Weltbank 2007

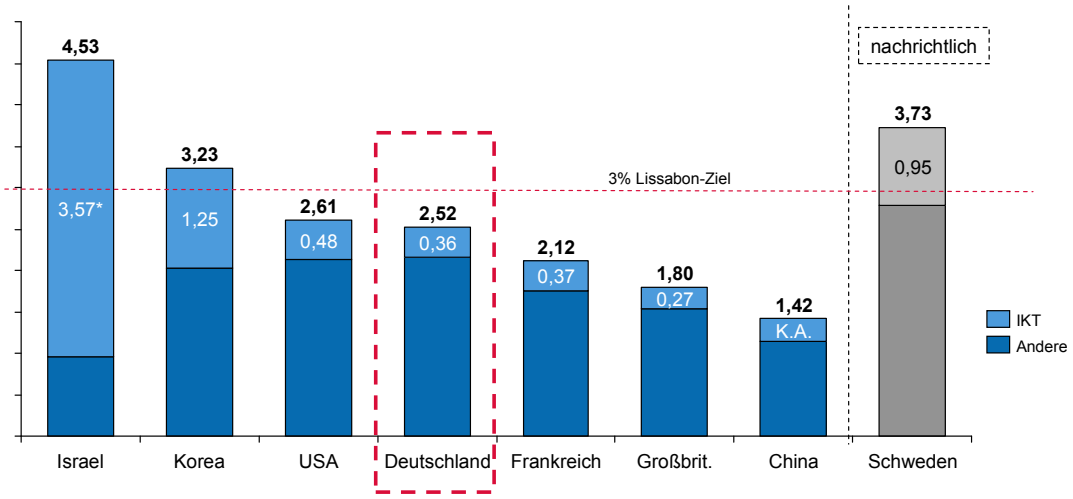


Abbildung 40: Übersicht der FuE-Ausgaben 2006 in Prozent des BIP (mit dem Anteil der öffentlichen Förderung)[146]

Im Folgenden werden die Vergleichsländer einzeln vorgestellt. Dabei werden wesentliche Aspekte des IT-Sicherheitsmarktes mit Blick auf die ordnungspolitischen Handlungsziele Sicherung kritischer Kompetenz, Innovation und Wachstum herausgestellt.

7.4.1 Republik Korea

Die Hersteller von Informations- und Kommunikationstechnologie in der Republik Korea tragen 16,1% zum Bruttoinlandsprodukt bei (2006). Mit über 30% ist die IKT-Industrie einer der größten Exportsektoren des Landes. Die Republik Korea legt den Schwerpunkt ihrer Aktivitäten eindeutig auf das Wachstum. Die geopolitische Lage des Landes bringt darüber hinaus besondere Herausforderungen an die nationale Sicherheit mit sich, an der die IT-Sicherheit einen bedeutenden Anteil hat.

Sicherung

Die Regierung hat im September 2009 einen umfassenden Plan zur Verbesserung der Internetsicherheit beschlossen, nachdem das Land im Juli 2009 massiven DDoS-Angriffen ausgesetzt war, die Regierungsrechner, Banken und Internetserver erheblich beeinträchtigt haben.

[146] OECD, UNESCO, Trajtenberg 2005, Booz & Company-Analyse

Der Plan sieht vor, 3000 Polizeibeamte zu sogenannten „Cyber Sheriffs" auszubilden, dem nationalen Nachrichtendienst die Federführung bei der Abwehr von Angriffen zu übertragen und bei der nationalen Armee eine separate Einheit aufzustellen, die sich mit Bedrohungen befassen soll, die von ausländischen Armeen ausgehen. Zusätzlich beinhaltet der Plan eine großangelegte Informations- und Aufklärungskampagne zur Verbesserung des Sicherheitsbewusstseins der Bevölkerung.

Darüber hinaus wird die Regierung die bestehenden Gesetze überprüfen, um die Überwachung der Netze zu verbessern, sowie die Staatsausgaben für IT-Sicherheit anheben.

Offensichtlich hat die Regierung erkannt, dass die IT-Sicherheit bislang nicht ausreichend beachtet wurde und das Land mit seiner sehr hohen Breitband-Penetrationsrate nur unzureichend geschützt ist.

Wachstum

Die Regierung hat schon Anfang der 90er Jahre die Weichen für den Erfolg der IKT-Industrie gelegt, und zwar durch

- konsequente Marktliberalisierung,
- die Anwendung internationaler Standards zur Erhöhung der Wettbewerbsfähigkeit und des Zuflusses ausländischer Investitionen sowie
- die Bündelung der Regierungstätigkeit im Ministerium für Information und Kommunikation (MIC).

Die Regierung verfolgt das Ziel, Korea zum IKT-Knotenpunkt in Nordostasien auszubauen. Hierzu wurde die Regierungsstrategie u-IT839 für die Jahre 2006–2010 verabschiedet. Diese Strategie hat zum Ziel, in diesem Zeitraum acht neue Dienste (u. a. HSDPA/W-CSMA, WiBro, RFID) zur Verfügung zu stellen, drei neue Infrastrukturen aufzubauen (vor allem Breitband), und neun neue Produkte (überwiegend Multimedia und Embedded Systems) zu entwickeln.[147]

Die Republik Korea konzentriert ihre IKT-Förderung auf wenige Global Player (z. B. Samsung, LG) und wenige IKT-Cluster (Digital Multimedia City, Nu-

[147] „New „u-IT839" Strategy Looks to the Future", Korea IT Times, 31. März 2006

ritkum und Songdo U-IT Cluster). Dadurch hat sich eine weltweit konkurrenzfähige Industrie entwickelt, die im Halbleiter-, TFT-LCD- und Mobiltelefonbereich zur Weltspitze zählt und über 11% der arbeitenden Bevölkerung beschäftigt.

2008 hat die Regierung einen Masterplan zur Stärkung der IT-Sicherheitsindustrie verabschiedet. Bis 2013 wird die Regierung rund 230 Mrd. Won (ca. 130 Mio. Euro) überwiegend in FuE investieren mit der Absicht, den heimischen Markt für IT-Sicherheit von derzeit 3,1 Billionen Won (ca. 2 Mrd. Euro) auf 18,4 Billionen Won (ca. 10 Mrd. Euro) auszubauen und 30.000 neue Arbeitsplätze zu schaffen. Der Weltmarktanteil koreanischer Hersteller für IT-Sicherheit soll von derzeit 1,74% auf ca. 5% gesteigert werden.

Industrieseitig wurden 2009 ebenfalls die Kräfte gebündelt und diverse (IITA, KIPA, KIEC) Agenturen in eine zentrale Organisation zusammengeführt, die nunmehr sehr umfassend und zentral für die IT-Sektorförderung in Korea zuständig ist: NIPA – National IT Industry Promotion Agency.

Die NIPA unterstützt die Regierung beim Entwurf von mittel- bis langfristigen FuE-Strategien für die IKT. Zur Unterstützung der KMU-Landschaft in Korea hält die NIPA verschiedene Finanzierungsinstrumente bereit, einschließlich Risikokapital. Darüber hinaus unterstützt die NIPA den Aufbau einer Open-source-basierten Softwareindustrie in Korea, um die Abhängigkeit von ausländischen Anbietern zu reduzieren. Bei der Exportförderung verfolgt die NIPA das Ziel, den Export koreanischer IKT bis 2012 auf 11 Mrd. US-Dollar zu steigern.

Fazit

Korea hat im Vergleich zu Deutschland den Aufbau der IT-Industrie und der IKT im Land massiv gefördert. Mit dem ambitionierten IT-Sicherheits-Masterplan wird dies nun über die nächsten Jahre auf die IT-Sicherheitsindustrie ausgedehnt. Korea kann dabei auf eine vollständige IKT-Basisinfrastruktur zurückgreifen. Die Regierung hat dabei die Entwicklung und die internationale Wettbewerbsfähigkeit einiger weniger nationaler Champions wie LG und Samsung gefördert und die Forschungsförderung auf wenige IT-Cluster konzentriert.

7.4.2 China

Die Volksrepublik China ist mit Abstand der größte Exporteur von IKT, gefolgt von den Vereinigten Staaten. Chinas Wachstum im IKT-Bereich wird im Wesentlichen getrieben vom Aufbau und der Nachrüstung des Telekommunikationsbereichs. Im internationalen Ranking der Breitband- und Internetverfügbarkeit belegt das Land jedoch weiterhin hintere Plätze. Die Gesamtausgaben für IKT machten 2007 7,2% des BIP aus. Unternehmen in China gaben in 2007 etwa 19% ihrer IT-Ausgaben für IT-Sicherheit aus, in den Vereinigten Staaten waren es im gleichen Zeitraum lediglich 12%. Als Grund dafür gilt der Nachholbedarf in China in Punkto Informationssicherheit und Informationsmanagement. Die chinesischen Unternehmen überwachen den E-Mail-Verkehr und die Internetnutzung ihrer Mitarbeiter weniger, als das in den USA üblich ist. Infolgedessen waren 70% der chinesischen Unternehmen in 2006 von Viren-Angriffen betroffen, in den USA „nur" 49%.[148]

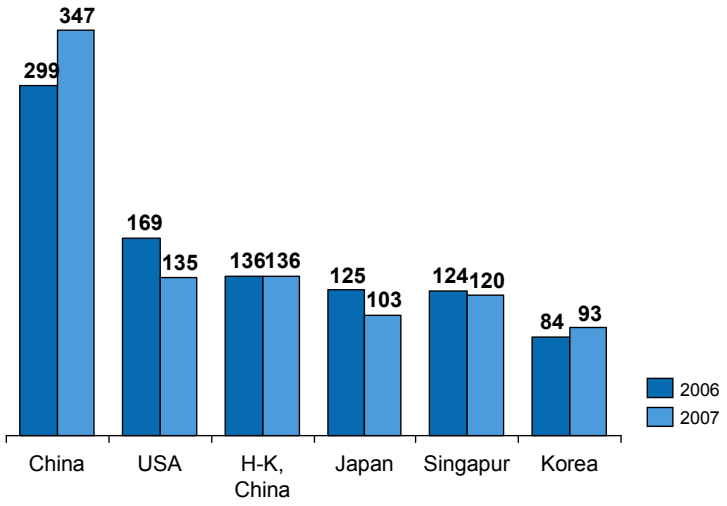


Abbildung 41: Die größten IKT-Exportländer der Welt (in Mrd. US-Dollar)[149]

Sicherung

Auf der Ebene des Staates hat man auf die wachsende Bedeutung des Themas IT-Sicherheit dadurch reagiert, dass die kommunistische Partei Chinas im Jahr 2004 die IT-Sicherheit auf eine Stufe mit politischer Stabilität, wirtschaft-

[148] Accenture und InformationWeek, Befragung von über 3000 IT- und Security-Fachleuten in China und den USA, 2007

[149] WTO

licher Sicherheit und der nationalen Verteidigung gestellt hat. Daraus haben sich die folgenden strategischen IT-Sicherheitsziele und -maßnahmen ergeben:

- Stärkung der führenden Rolle der Regierung auf verschiedenen Ebenen der IT-Sicherheit und vollständige Anwendung der strategischen Prinzipien der Zentralregierung auf die IT-Sicherheit,
- Stärkung der Grundlagen zur Verbesserung der Fähigkeiten für eine nachhaltige Entwicklung von IT-Sicherheit (einschließlich Schaffung eines umfassenden IT-Sicherheitsrechts, von IT-Sicherheitsstandards sowie eines Informations- und Schulungssystems zum Thema IT-Sicherheit),
- Beschleunigung des Aufbaus einer heimischen Industrie für IT-Sicherheitstechnologie,
- aktive Teilnahme an der internationalen Zusammenarbeit, insbesondere beim Kampf gegen grenzüberschreitende Internetkriminalität,
- Verabschiedung effektiver Maßnahmen zur Verbesserung des Sicherheitsschutzes der Basis-Netzinfrastruktur und wichtiger Informationssysteme (einschließlich der Regulierung von Schutzniveaus bei der IT-Sicherheit, der Abgrenzung der Zuständigkeiten der Behörden, der Systemhersteller, und der Betreiber sowie des Aufbaus eines Meldewesens und eines Notfallsystems für die IT-Sicherheit).[150]

Die Aufsichtsbehörde für IT-Sicherheit (Chinese Public Security Public Information Network Security Supervisory Bureau) veröffentlicht auf der Internetseite www.infosec.org.cn die aktuellen IT-Sicherheitsnormen sowie Sicherheitsmeldungen und Virenwarnungen.

China verfügt mit dem China National Information Security Testing, Evaluation and Certification Center (CNISTECC) über eine regierungsnahe nationale Zertifizierungsorganisation. Die Zertifizierung durch das CNISTECC erfolgt eigenen Angaben zufolge nach den einschlägigen internationalen ISO- und IEC-Standards. Weiterhin wird die Einhaltung der amerikanischen Standards angestrebt, um Konformität mit dem WTO-Regelwerk zu gewährleisten.

[150] „IT SECURITY IN THE USA, JAPAN AND CHINA", Studie des Swedish Institute for Growth Policy Studies, 2005

Das CNISTECC führt zudem Risikoüberprüfungen für Regierung und Unternehmen hinsichtlich der kritischen Infrastruktur durch.

Im Rahmen dieser Studie wurde von manchen Unternehmen die fehlende Transparenz dieses Zertifizierungsverfahrens kritisiert. Die bei Zertifizierungen international nicht unübliche Verpflichtung, das Quellprogramm (Source Code) offenzulegen, wird deshalb als unkalkulierbares Risiko angesehen, zumal die Offenlegung in China die Einfuhrfähigkeit des Produkts in anderen Ländern beeinträchtigen kann. China ist derzeit weder dem Abkommen über die gegenseitige Anerkennung von IT-SEC-Zertifikaten beigetreten, noch nimmt es an den Common Criteria Agreements (CCRA) über die gegenseitige Anerkennung von Zertifikaten nach dem Common-Criteria-Standard teil. Ein Beitritt Chinas zu diesen Vereinbarungen könnte die Problematik des Technologietransfers beheben. Der CC-Standard ist bereits ins Chinesische übersetzt worden, und Vertreter Chinas haben die nationalen Zertifizierungsstellen in vielen Ländern besucht, unter anderem das NIST in USA, das CESG in Großbritannien, die IPA in Japan und die KISA in Korea (allerdings nicht das BSI), und China prüft ferner eine mögliche Teilnahme am CCRA.[151]

Innovation

Mit ihrem 11. Fünf-Jahres Plan (2006–2010) investiert die Volksrepublik insgesamt 6 Mrd. RMB (ca. 600 Mio. Euro) in zwölf große Wissenschafts- und Technologieprojekte. Zusätzlich werden 5 Mrd. RMB (ca. 500 Mio. Euro) für Phase III des „knowledge innovation project" zum Aufbau von 50 nationalen Entwicklungsforschungszentren und 100 nationalen Entwicklungslabors und zum Bau von 300 industriellen Technologiezentren sowie weiteren Infrastrukturprojekten zur Verfügung gestellt.

Wachstum

China hat seine IT-Industrie in den Zentren Peking/Tianjin, East und Guandong konzentriert. Daneben treibt die Regierung den Bau des „China International ICT Innovation Cluster (CIIIC)" voran. Mit Hilfe der Ansiedlung aus-

[151] CC in China, Zhuohui Liu CNCA, Xiaohua Chen ISCCC, September 2008

ländischer Firmen und Forschungseinrichtungen aus den Vereinigten Staaten, Japan und Europa soll das CIIIC zur größten IKT-Zone Asiens werden.

Von diesen Investitionen in die IKT-Infrastruktur des Landes profitiert auch die IT-Sicherheitsindustrie. Die Rising Corp., der größte inländische Hersteller von IT-Sicherheitstechnologie, hat weltweit konkurrenzfähige Produkte wie die RSW-2000, eine ASIC-Chip-basierte Firewall, auf den Markt gebracht.

Fazit

Wie in vielen anderen Technologiebereichen setzt China auch bei der IT-Sicherheit auf Technologietransfer. Die Ausfuhr von IT-Sicherheitstechnologie nach China stellt für Hersteller ein Risiko des ungewollten Technologietransfers dar, da die intransparente und verpflichtende Zertifizierung der Produkte vor der Einfuhr die Offenlegung des Quellcodes erfordert.

Auf der anderen Seite bietet der chinesische Markt einen attraktiven Markt für IT-Sicherheitsprodukte, die sich (für die vielen Unternehmen mit Produktionsstätten in China) auf den Schutz des geistigen Eigentums spezialisieren. Darüber hinaus bietet China einen attraktiven und großen Markt für Massenprodukte der IT-Sicherheit (z. B. Antivirus, Firewalls), der das Risiko der Zertifizierung wert sein kann.

7.4.3 USA

Die Vereinigten Staaten sind der größte IT-Markt weltweit mit einem Anteil am Weltmarkt von über 28% gemessen an den Umsatzzahlen für 2008. Darüber hinaus sind die USA (nach China) der zweitgrößte IKT-Exporteur der Welt (vgl. Abbildung 5). Diese dominante Stellung spiegelt sich auch im IT-Sicherheitsbereich wider. Auf der Liste der weltweit führenden Anbieter von IT-Sicherheitstechnologie finden sich auf den ersten zehn Plätzen ausschließlich amerikanische Unternehmen.[152]

[152] Worldwide IT Security Software, Hardware , and Services 2009-2012 Forecast and 2007 Vendor Shares, IDC, 2009

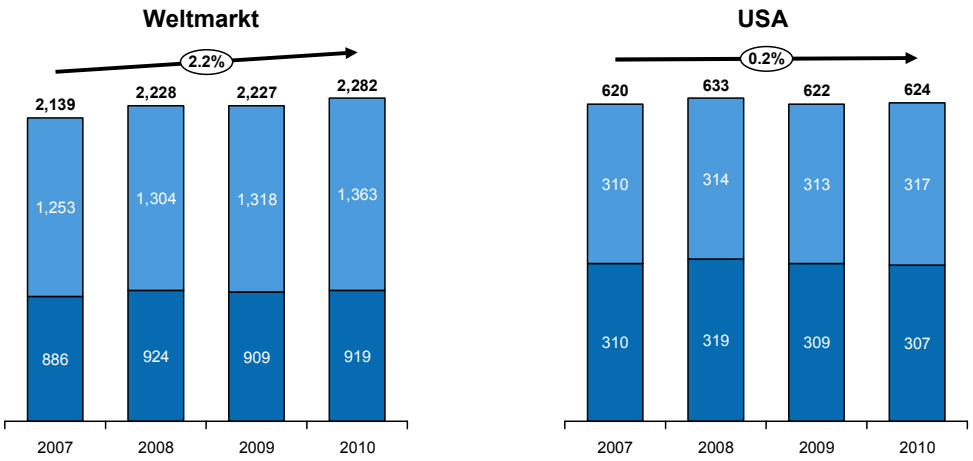


Abbildung 42: Überblick der IKT-Umsätze 2007–2009 (Marktwert in Mrd. Euro)[153]

Dies ist unter anderem ein Ergebnis der geringen Neigung der amerikanischen Regierung, den Markt zu regulieren. Dies fördert den freien Wettbewerb, eine hohe Investitionsbereitschaft und die Forschungselite. Hingegen hat der amerikanische Staat ein sehr stark ausgeprägtes Sicherheitsbestreben, sich gegen Angriffe jeder Art von außen zu schützen. Demgemäß ist der Staat ein bedeutender Nachfrager von IT-Sicherheit, tritt als Vermittler amerikanischer Sicherheitstechnologie im Ausland auf und agiert als Wächter amerikanischer Schlüsselindustrien in Bezug auf kritische Infrastrukturen.

Sicherung

Die US Regierung hatte 2008 unter der Bush-Administration die „Comprehensive National Cyber Security Initiative (CNCI)“ als National Security Presidential Directive 54/Homeland Security Presidential Directive 23 verabschiedet. Diese Initiative ist als „streng geheim“ eingestuft, und nur wenige Details sind bekannt. Gerüchteweise ist das Programm mit einem Gesamtbudget von 30–40 Mrd. US-Dollar (6–8 Mrd. pro Jahr) ausgestattet.

Das „Trusted Internet Connections Programm” ist die bislang bekannteste und am weitesten fortgeschrittene Initiative aus dem CNCI-Programm. Das Verwaltungs- und Haushaltsamt (Office of Management and Budget – OMB) hat dieses Programm im November 2007 entworfen mit dem Ziel, die Anzahl der Netzzugänge von den Bundesbehörden in externe Computernetze auf un-

[153] EITO 2009 (rel. August 2009)

ter 100 zu reduzieren. Von Januar bis Mai 2008 konnte die Anzahl bereits von 4300 auf etwa 2750 verringert werden.

Der Grundgedanke dieses Programm ist, die Überwachung der Netzzugänge zu erleichtern und die Wahrscheinlichkeit der Aufdeckung einer Sicherheitslücke zu erhöhen. Zur Überwachung der Netzzugänge wurde ein einheitliches System entwickelt, welches von allen Bundesbehörden verpflichtend einzusetzen ist und das U. S. Computer Emergency Readiness Team über Vorfälle informiert.

Die Obama-Administration hat mittlerweile ein Cyber Security Policy Review durchgeführt, das mit kurzfristigen Maßnahmen die nationalen Anstrengungen bei der Sicherheit des virtuellen Raums (Cyber-Security) verbessern soll:

1. Schaffung der Stelle des nationalen Cyber-Security-Beraters, welche direkt an den Präsidenten berichtet und für die Koordinierung der Tätigkeiten aller Bundesbehörden (u. a. FBI, NSA, Pentagon, Heimatschutzministerium) sowie für die Grundsatzfragen der nationalen Cyber Security zuständig sein wird.

2. Initiierung von **FuE-Anstrengungen zu „Safe Computing"** und Verstärkung der nationalen Cyber-Infrastruktur**.**

3. Zusammenarbeit mit dem privaten Sektor zur Schaffung neuer Standards im Hinblick auf die Web-Sicherheit und die physikalische Belastbarkeit zum **Schutz der IT-Infrastruktur**.

4. Zusammenarbeit mit der Industrie zur Entwicklung der notwendigen Systeme zum **Schutz von Handelsgeheimnissen und FuE-Ergebnissen vor Industriespionage**.

5. Entwicklung einer **Strategie gegen Internet-Kriminalität** zur Minimierung des Potenzials krimineller Gewinne.

6. Vorgeben von Standards zur Sicherung von persönlichen Daten und Verpflichtung der Unternehmen, datenschutzrelevante Vorfälle zu melden.

Innovation

Mit dem „**Cyber Security Research & Development Act**" aus dem Jahr 2002 wurden der „National Science Foundation (NSF)" und dem „National Institute of Standards and Technology (NIST)" für einen Zeitraum von fünf Jahren über 880 Mio. US-Dollar für Forschungsvorhaben aus dem Bereich der Web-

Sicherheit zugewiesen. Das NSF förderte mit dem Geld den Aufbau neuer Cyber Security Forschungszentren und Stipendien. Das National Institute of Standards and Technology (NIST) förderte mit dem Geld Partnerschaften zwischen Forschung und Industrie und konnte erfahrene Forscher aus anderen Gebieten für die Forschung auf dem Gebiet der IT-Sicherheit gewinnen.

Die 2008 verabschiedete **„Comprehensive National Cybersecurity Initiative (CNCI)"** ist ein neues, streng geheimes Regierungsprogramm zur Förderung der Entwicklung neuer Technolgien für die IT-Sicherheit. Aus diesem Programm finanziert sich u. a. das **National Cyber Range Programm** der DARPA (Defense Advanced Research Projects Agency), welches die Forschungs- und Entwicklungsaktivitäten der Regierung im Hochrisikobereich und bei der Zusammenarbeit mit Partnern aus der Wirtschaft vorantreibt, und zwar im Sinne einer technischen Neugestaltung der virtuellen Umgebung.

Daneben wurde mit der Schaffung des Heimatschutzministeriums (DHS) ein weiteres FuE-Programm für Cyber Security geschaffen. Im Jahr 2007 standen dem DHS 23 Mio. US-Dollar für Forschungsvorhaben zur Verfügung. Das DHS betreibt das „**Cyber Security R&D Center**" in enger Zusammenarbeit

- mit der IT-Sicherheitsindustrie – zur Durchführung und Koordinierung von FuE-Aktivitäten der öffentlichen und privaten Hand,
- mit Wagniskapitalgebern, um FuE-Ergebnisse und daraus hervorgehende Produkte an den Markt zu bringen und
- mit dem Bildungswesen – zur Verbesserung des Sicherheitsbewusstseins und zur Erhöhung der Zahl der IT-Sicherheitsfachkräfte.

Mit dem **Silicon Valley** verfügen die USA über das bekannteste und erfolgreichste IT-Technologiezentrum bzw. -Cluster. Die günstigen Voraussetzungen – staatliche Unterstützung, unmittelbare Nachbarschaft zur Stanfort University und Verfügbarkeit von Wagniskapital – haben die Weltmarktstellung amerikanischer IT-Unternehmen ermöglicht.

Als weiterer wichtiger Aspekt, der Innovationen in der IT-Sicherheitsbranche fördert, wurde von im Rahmen dieser Studie befragten Unternehmen das öffentliche Vergabeverfahren in den USA hervorgehoben. Sie erklärten, dass dieses Verfahren die Wettbewerbsteilnahme großer wie kleinster Anbieter ermögliche und somit viel Gelegenheit biete, innovative Ideen und Lösungen vorzuschlagen. So werden bei großen Beschaffungsvorhaben häufig mehrere

Auswahlrunden durchgeführt, bei denen es am Anfang mehr auf die Idee ankommt als auf die Fähigkeit zu einer flächendeckenden Implementierung.

Wachstum

Die USA haben mit „**Export.gov**" ein zentrales Regierungsportal unter Federführung der Behörde für internationalen Handel des amerikanischen Wirtschaftsministeriums geschaffen, bei dem über 19 Regierungsbehörden zusammenarbeiten, um amerikanische Unternehmen bei der Planung ihrer Exportstrategien zu unterstützen, und sich aktiv um den Erfolg dieser Unternehmen in internationalen Märkten bemühen. „Export.gov" wird vom amerikanischen Wirtschaftsdienst verwaltet (Abteilung für Wirtschaftsförderung der Behörde für internationalen Handel). Der Wirtschaftsdienst verfügt über Büros mit Wirtschafts- und Handelsexperten in 107 amerikanischen Städten und in den amerikanischen Botschaften in über 80 Staaten. Die Dienstleistungen umfassen

- weltweite Marktforschung,
- Messen und Veranstaltungen zur Vermarktung der Produkte und Dienstleistungen an qualifizierte Abnehmer,
- Vermittlung und Geschäftsanbahnung mit qualifizierten Käufern und Händlern und
- Beratung und rechtliche Unterstützung bei allen Schritten des Exportverfahrens.

Fazit

Die Vereinigten Staaten zeichnen sich durch eine hohe Dienstleistungsorientierung des Staates aus, die insbesondere auch der IT-Sicherheitsindustrie zugutekommt. Durch die Zusammenarbeit der verschiedenen Regierungsstellen im Inland und die Einbindung der Botschaften im Ausland haben amerikanische Unternehmen bei der Vermarktung sicherheitsrelevanter Produkte und Dienstleistungen bei ausländischen Regierungen einen entscheidenden Vorteil gegenüber deutschen Unternehmen, die im Wesentlichen lediglich auf nicht-staatliche Organisationen wie die Auslandshandelskammern zurückgreifen können.

Im Übrigen hat der Staat mit der Cyber-Security-Strategie und der Schaffung einer zentralen Regierungsstelle im Weißen Haus der IT-Sicherheit höchste Priorität eingeräumt und die Zuständigkeiten innerhalb der Regierung neu geordnet. Zudem tritt der Staat konsequenter als Abnehmer von IT-Sicherheitsprodukten auf, da die Einhaltung von Sicherheitsstandards in der öffentlichen Verwaltung Pflicht ist (und nicht nur Empfehlung wie in den meisten Fällen in Deutschland). Die neuen Aufgaben des BSI sowie die Möglichkeiten des IT-Rats, Sicherheitsstandards vorzuschreiben, können in diesem Punkt allerdings eine rasche Änderung herbeiführen.

Die USA haben darüber hinaus mit dem größten Wagniskapitalmarkt weltweit und einer sehr engen Zusammenarbeit zwischen Industrie und Forschung optimale Rahmenbedingungen, insbesondere für innovative und junge Unternehmen, die Entwicklung neuer Produkte und Hochsicherheitstechnologie finanziell zu unterstützen.

7.4.4 Frankreich

Ähnlich wie Deutschland verwendet Frankreich etwas mehr als 2% seines Bruttoinlandsprodukts für FuE-Ausgaben. Dies und die geographische Nähe macht Frankreich im Ländervergleich besonders relevant.

Sicherung

Die neue Nationale Agentur für die Sicherheit von Informationssystemen (ANSSI) wurde im Juli 2009 durch den Zusammenschluss der ehemaligen ANSSI und der ehemaligen zentralen Direktion für die Sicherheit von Informationssystemen (DCSSI) gegründet. Die Agentur ist dem französischen Verteidigungsministerium zugeordnet. Vorangegangen war die Veröffentlichung des Weißbuches über die Verteidigung und nationale Sicherheit 2008, in dem die Bedeutung der Cyber-Bedrohungen hervorgehoben wurde. Das Weißbuch hatte die Notwendigkeit erkannt, eine zentrale Stelle zum Schutz der IKT als kritischer Infrastruktur in Frankreich zu schaffen.

Die ANSSI hat unter anderem die folgenden Aufgaben:

- Früherkennung von Angriffen durch laufende Überwachung der sensiblen Netze und Durchführung von Abwehrmaßnahmen,
- nationale Zertifizierungsstelle für IT-Sicherheitsprodukte,

- Beratung und Unterstützung für Regierung und Unternehmen,
- Öffentlichkeitsarbeit über die IT-Sicherheit.

Innovation

In 2009 hat Frankreich die nationale Strategie für Forschung und Entwicklung überarbeitet, um dem Lissabon-Ziel von 3% des BIP für Forschung und Entwicklung näherzukommen.

Die „Stratégie nationale de recherche et d'innovation" sieht die Forschung in der IKT (insbesondere in der IT-Sicherheit) und Nanotechnologie als eines der Kernthemen für die Forschungsförderung. Die Strategie nimmt dabei direkt Bezug auf die großen französischen Unternehmen (z. B. France Telecom, Alcatel Lucent, Bull, Thales, Dassault) und hebt deren Bedeutung für die Stellung Frankreichs im Bereich der Forschung und IKT-Entwicklung hervor, insbesondere im Verteidigungsbereich.

Die Regierung betreibt unter „http://www.securite-informatique.gouv.fr/„ ein Informationsportal für Bürger und Unternehmen, auf dem unter anderem über aktuelle Bedrohungen und Sicherheitslücken informiert wird. Es werden auch Onlinekurse zu IT-Sicherheitsthemen angeboten sowie CESG-zertifizierte Produkte in einer Datenbank hinterlegt.

Wachstum

Frankreich hat ähnlich wie die Vereinigten Staaten eine sehr stark staatsgetriebene Außenwirtschaftsförderung. Wichtigster Akteur in der Außenwirtschaftsförderung sind die Wirtschaftsmissionen (missions économiques), die sowohl dem Wirtschafts-, Finanz- und Beschäftigungsministerium als auch den Botschaften unterstehen und organisatorisch in die Botschaften direkt integriert sind. Der Schwerpunkt der Missionen liegt auf der konkreten Unterstützung von meist großen Unternehmen vor Ort und auf der Beschaffung, Analyse und Verbreitung von Informationen.

Als zentrale Anlaufstelle für Informationen, Kontakte und Vermittlungen für Unternehmen in Frankreich hat der Staat mit Ubifrance ein öffentliches Unternehmen gegründet, welches Angebote der Wirtschaftsmissionen sowie anderer öffentlicher Stellen bündelt und den Unternehmen als Wegweiser dient. Zudem hat Ubifrance ein breites Netzwerk öffentlicher und privater Akteure

aufgebaut, das ein gebündeltes „Export-Know-how“ anbietet (unter Einschluss von Schulungsanbietern).

Zur Unterstützung französischer KMUs hat der Staat 2006 das Programm CAP EXPORT aufgelegt, das mit Steuererleichterungen und Exportkrediten die im internationalen Vergleich geringe Exportquote der französischen KMUs steigern will.

Fazit

Im Gegensatz zu Deutschland verpflichtet sich Frankreich nicht zur Neutralität und Objektivität, wenn es um die Unterstützung der französischen Wirtschaft geht. Insbesondere im Handel mit sicherheitsrelevanten Produkten und Technologien wie in der IT-Sicherheit verschafft der französische Staat den französischen Unternehmen durch seine starke staatliche Beteiligung bei der Anbahnung und beim Abschluss von Geschäften im Ausland einen entscheidenden Wettbewerbsvorteil.

Die französische Wirtschaftsstruktur, die von zahlreichen international führenden Großunternehmen geprägt ist, spiegelt sich auch in der französischen IT-Sicherheitsbranche wider, in der Unternehmen wie Thales sehr stark mit dem Rüstungsgeschäft verbunden sind. Diese enge Verzahnung spiegelt sich auch in der französischen IT-Sicherheitsstrategie wider, die Teil der übergeordneten nationalen Sicherheitsstrategie ist und bei der die ANSSI als Hauptakteur dem französischen Verteidigungsministerium untersteht.

Allerdings geht diese Förderpolitik zu Lasten der KMUs, die trotz der Fördermaßnahmen im internationalen Vergleich eine geringe Exportquote aufweisen.

7.4.5 Vereinigtes Königreich (VK)

Das Vereinigte Königreich wendet mit 6,7% des BIP an IKT-Ausgaben im direkten Vergleich mit Deutschland deutlich mehr für IKT auf. Hinzu kommt, dass der Exportanteil der IKT-Güter an den Gesamtausfuhren mit 21% deutlich höher liegt als in Deutschland mit 10%. Im Vergleich der internationalen Rankings liegt das VK an der europäischen Spitze und in allen wesentlichen Aspekten deutlich vor der Bundesrepublik.

Sicherung

Das Vereinigte Königreich hat im Juli 2009 im Rahmen der jährlichen nationalen Sicherheitsstrategie erstmalig eine nationale Cyber-Security-Strategie verabschiedet. Diese ist Teil der übergeordneten „Digital Britain"-Strategie. Auf der Grundlage der Cyber-Security-Strategie werden zwei neue Regierungsstellen geschaffen, zum einen das OCS (UK Office of Cyber Security) und zum anderen das CSOC (UK Cyber Security Operations Centre). Beide Behörden sollen bis Ende März 2010 ihre Arbeit aufnehmen und berichten direkt der Abteilung Information Security and Assurance (IS&A) des Cabinet Office.

Während dem OCS die strategische Federführung für Fragen der Cyber Security innerhalb der Regierung zukommt, wird das CSOC, ähnlich dem BSI in Deutschland, eher operationelle Aufgaben übernehmen und Aufklärungsarbeit leisten. Insbesondere wird das CSOC die Sicherheit des Internets überwachen und die Maßnahmen zur Behebung von Störungen koordinieren.

Für den Schutz der kritischen Infrastruktur ist zentral das CPNI (Centre for the Protection of National Infrastructure) zuständig, welches im Bereich der Informationsinfrastruktur aber mit dem CESG (UK's National Technical Authority for Information Assurance) und künftig auch mit dem OCS und dem CSOC zusammenarbeiten wird. Beim CESG ist das britsche Computer Emergency Response Team (CERT) untergebracht, dessen Aufgaben in Deutschland ebenfalls vom BSI wahrgenommen werden.

Das CESG fördert unter anderem privatwirtschaftliche Unternehmen bei der Entwicklung von Krypto-Produkten (CESG Assisted Products Service (CAPS)) und führt Zertifizierungen durch. Das CESG betreibt zudem eine Datenbank, in der ausschließlich die mit eigenen CAPS-Zertifikaten versehenen Produkte gesucht werden können.

Innovation

Mit der übergeordneten Strategie „Digital Britain" hat die Regierung eine umfassende Analyse der Rolle der IKT im Vereinigten Königreich vorgenommen. Das Hauptanliegen dieser Strategie ist es, die führende Stellung des Landes in den Wirtschaftsbereichen Wissen und Lernen zu festigen, und zwar durch folgende Maßnahmen:

- Modernisierung und Ausbau der Festnetz-, Mobil- und Rundfunk-Infrastruktur,

- günstige Rahmenbedingungen für Investitionen in und Innovationen bei digitalen Inhalten, Anwendungen und Diensten,
- Bereitstellung von hochwertigen und aktuellen Informationsangeboten im Internet seitens der öffentlichen Verwaltungen,
- Entwicklung der digitalen Fertigkeiten des Landes auf allen Ebenen und
- Sicherstellung des Zugangs zu Breitbandnetzen, Erhöhung der Anzahl der Breitbandanschlüsse und Einsatz von Breitband zur effektiveren und effizienten Bereitstellung von öffentlichen Diensten.

Für das Digital-Britain-Programm wurde ein umfangreicher Implementierungsplan erstellt. Im Bereich Forschung und Ausbildung werden in den kommenden drei Jahren im Rahmen des Digital Economy Programme 120 Mio. Brit. Pfund zur Verfügung gestellt. Hinzu kommen weiter 30 Mio. Brit. Pfund für Innovationsprojekte über das Technology Strategy Board (TSB). Darüber hinaus hält das TSB einen Innovation Investment Fund bereit, der mit 150 Mio. Brit. Pfund für Forschung und Entwicklung in neuen Technologien ausgestattet ist, jedoch kein gesondertes Programm zur Förderung der IT-Sicherheit enthält.

Wachstum

Zuständig für die Förderung von IT-Sicherheit in der Wirtschaft und als Branche ist das Department for Business Innovation & Skills (BIS). Das Information Security Policy Team des BIS wirbt aktiv für die Anwendung internationaler Sicherheitsstandards in britischen Unternehmen, welche sich häufig unzureichend mit der IT-Sicherheit auseinandersetzen.

Das BIS beschreibt die britische IT-Sicherheitsbranche als einen wesentlichen Treiber bei der Entwicklung wichtiger IT-Sicherheitsstandards. Bislang sei jedoch kein Unternehmen mit signifikanter Marktstellung entstanden. Der britische IT-Sicherheitsmarkt sei sehr zersplittert, sowohl auf der Anbieter- als auch auf der Nachfragerseite.

Die vom Technology Strategy Board des BIS erarbeitete Strategie für die Förderung von Forschung und Entwicklung in der IKT enthält keine konkreten Pläne, die Situation der britischen IT-Sicherheitsbranche zu verbessern. Zwar enthält die Strategie den Bereich Netzwerksicherheit, aber diese stellt keinen

erkennbaren Schwerpunkt dar. Eine von der britischen Regierung zusammen mit Industriepartnern betriebene Ratgeber-Website für Heimanwender und Business (getsafeonline.org) rät diskriminierungsfrei zu Softwarelösungen der internationalen Marktführer (u. a. F-Secure, Kaspersky, McAfee, Microsoft, Trend Micro, Symantec). Insgesamt sind für den IT-Sicherheitsbereich keine „Buy UK"-Taktiken erkennbar.

Die Außenwirtschaftsförderung zugunsten britischer Unternehmen erfolgt über die staatliche Einrichtung „UK Trade and Investment" (UKTI). Das UKTI hat eine hohe Dienstleistungsorientierung und zeichnet sich durch einen „One-face-to-the-customer"-Ansatz für die britischen Unternehmen, durch hohe Kompetenz der Experten sowie durch klare qualitative und quantitative Zielvorgaben (mit Berichterstattung über die Zielerreichung) aus.

Alle Botschaften verfügen über eine Handelsabteilung bzw. eine Trade & Investment-Abteilung (die dann mit UKTI-Mitarbeitern besetzt ist) mit mehreren Mitarbeitern, wobei der Fokus auf Ländern und Branchen mit großem Potenzial liegt, insbesondere auf der Hightech-Industrie sowie auf Forschung und Entwicklung.

Im Allgemeinen unterstützt die Regierung die britische Wirtschaft sehr offensiv. So veranstaltete kürzlich das Home Office eine große Informationsveranstaltung zum Thema Sicherheitsforschung im 7. EU Rahmenprogramm, bei dem hochrangige Vertreter der EU eingeladen waren und zu Fragen der Fördermaßnahmen und Antragsverfahren Stellung nahmen. Das Ziel dieser Veranstaltung war es, britische Unternehmen, Universitäten, Forschungseinrichtungen und Anwender zusammenzubringen und zu einer Teilnahme an diesem EU-Förderprogramm zu ermutigen.

Fazit

Für den Vergleich mit Deutschland ist vor allem die hohe Dienstleistungsorientierung der britischen Verwaltung bei der Außenwirtschaftsförderung herauszuheben. Zwar ist das Exportkreditwesen weit weniger entwickelt als in Deutschland, jedoch betätigt sich UKTI sehr stark bei der Investorenakquise für alle Firmen, die in Großbritannien investieren wollen. Der besondere Fokus liegt hierbei auf Unternehmen aus Hightech-Branchen und solchen, die in Großbritannien ihre Forschungs- und Entwicklungszentren aufbauen wollen.

Dem UKTI werden hierzu Zielvorgaben gemacht, die sich an der Höhe des akquirierten Kapitals und an der Zahl der dadurch geschaffenen Arbeitsplätze orientieren.

Im Hinblick auf die IT-Sicherheitsstrategie hat das Vereinigte Königreich, ähnlich wie die Vereinigten Staaten und Frankreich, zentrale Zuständigkeiten im Cabinet Office geschaffen, um eine wirksame Koordinierung der Regierungsarbeit in IT-Sicherheitsfragen zu gewährleisten.

7.4.6 Israel

Israel hat vor allem im IT-Sicherheitsbereich eine herausgehobene Stellung in der Welt. Dies ist unter anderem darauf zurückzuführen, dass Israel im direkten Vergleich mit den anderen Ländern, die in dieser Studie untersucht werden, mit 4,58% des BIP (2007) die höchsten Ausgaben für FuE leistet. Daneben gibt es weitere Faktoren, die die Entwicklung des IT-Standorts Israel beeinflusst haben. Laut einer Studie des Weltwirtschaftsforums (WEF) hat Israel über Jahre in die Bildung investiert sowie günstige Bedingungen für ausländische Investoren und Wagniskapitalgeber geschaffen.

Im Ergebnis hat Israel die höchste Pro-Kopf-Dichte an Ingenieuren. Mit 140 Ingenieuren pro 10.000 Beschäftigte hat Israel doppelt so viele wie die Vereinigten Staaten, die an zweiter Stelle folgen. Neben der Bildungspolitik hat der Zuzug von Millionen von Zuwanderern aus Osteuropa und der Sowjetunion nach 1989 hierzu beigetragen, unter denen über 100.000 gut ausgebildete Wissenschaftler und Ingenieure waren.

Sicherung

Im Bereich der IT-Sicherheit hat Israel 2006 durch die Zusammenlegung verschiedener bereits langjährig tätiger Regierungsbehörden unter dem Dach des Justizministeriums die „Israeli Law, Information and Technology Authority (ILITA)“ gegründet. Zu ihren Aufgaben gehört die Regulierung und Zertifizierung der elektronischen Signatur, die Verbesserung des Datenschutzes und die Bekämpfung von Datenschutzverstößen und sonstigen IT-gestützten Vergehen. Ferner fungiert sie als zentrales rechtliches Informationszentrum.

Im Übrigen fallen viele Aspekte der IT-Sicherheit in Israel unter die nationale Sicherheitsstrategie. Israel befindet sich im ständigen „Cyber War“ mit seinen

Gegnern, bei dem beide Seiten Propagandaangriffe auf Internetseiten der jeweils anderen Seite durchführen.[154] Viele Informationen über die IT-Sicherheitsstrategie Israels sind daher nicht zugänglich.

Innovation

Im Bereich Forschung und Entwicklung hat Israel frühzeitig entsprechende rechtliche Rahmenbedingungen und zentrale Regierungszuständigkeiten geschaffen. Zum einen hat das Land bereits in den 60er Jahren beim Ministerium für Industrie, Handel und Arbeit das Amt eines obersten Wissenschaftlers geschaffen (Office of Chief Scientist [OCS]), der bis heute die Fördermittel der Regierung für Forschung und Entwicklung verwaltet. Zum anderen hat Israel 1984 mit dem „Law for the Encouragement of Industrial Research & Development (LEIRD)" die rechtliche Grundlage geschaffen, die bis heute die staatliche Förderung von FuE der Industrie regelt. Das OCS verwaltet unter dem „Industrial Research & Development Program" ein Jahresbudget von 300 Mio. US-Dollar und fördert im Jahr an die 1000 Projekte von über 500 Firmen.

Daneben unterhält das OCS das „Technological-Incubator"-Programm, welches mit 30 Mio. US-Dollar im Jahr Cluster fördert, die sich mit FuE-Projekten befassen, die sich in einem sehr frühen und risikobehafteten Stadium befinden, wo häufig nicht mehr als eine vielversprechende Idee existiert. Insgesamt wurden 24 Cluster bzw. „technology incubators" aufgebaut, die jeweils rund zehn Projekte durchführen, die eine durchschnittliche Laufzeit von zwei bis drei Jahren haben.

Wachstum

Exportförderung sowie die Ansiedlung ausländischer Industrie wird als staatliche Aufgabe angesehen und mit umfangreichen Programmen unterstützt. Mit dem „Law for the Encouragement of Capital Investment (LECI)" hat Israel bereits Ende der 50er Jahre die rechtlichen Grundlagen dafür gelegt, die nach wie vor gültig sind.

Vor allem hat Israel Anfang der 90er Jahre mit dem „Yozma"-Programm die Ansiedlung von Wagniskapitalgebern mit 100 Mio. US-Dollar gefördert. Der-

[154] „Hamas office declares cyber-war on Israel", Los Angeles Times, 25. Oktober 2008

zeit ist Israel mit über 100 Wagniskapitalgebern und über 12 Mrd. US-Dollar an Wagniskapital aus den USA, Europa und dem Fernen Osten nach den USA der zweitgrößte Wagniskapitalmarkt der Welt. Das hat gemäß WEF mit 40% einen erheblichen Beitrag zum Wirtschaftswachstum Israels zwischen 1995 und 2004 geleistet.[155]

Fazit

Israel zeichnet sich insbesondere durch seine starke FuE-Förderung der IT-Industrie sowie durch seine optimalen Rahmenbedingungen für Wagniskapital aus. Die Bündelung der Zuständigkeiten im „Office of Chief Scientist" und die im Verhältnis zur Größe des Landes finanziell sehr gut ausgestatteten Förderprogramme haben den Aufbau der israelischen IT-Sicherheitsindustrie ermöglicht.

Die geopolitische Lage Israels bedingt zudem, dass die IT-Sicherheit – neben den zivilen Aspekten für die Bevölkerung und die Unternehmen – auch in der nationalen Verteidigung eine zentrale Rolle einnimmt.

[155] „Factors in the Emergence of an ICT Powerhouse", World Economic Forum, 2005

7.5 Die Notwendigkeit ordnungspolitischen Handelns für die IT-Sicherheitsbranche

Ordnungspolitisches Handeln in einem bestimmten Sektor bedarf einer Begründung. Im Bereich der IT-Sicherheit lässt sich diese aus drei Argumentationssträngen herleiten, die wiederum grundlegenden Handlungsziele entsprechen. Während dieser Abschnitt diesen Gesamtzusammenhang herausstellt, liegt das Hauptaugenmerk der konkreten Maßnahmenvorschlägen (7.6) auf den Handlungsoptionen für das BMWi.

Gesamtstaatliche Relevanz

Der Bereich IT-Sicherheit kann aufgrund seiner gesamtstaatlichen und volkswirtschaftlichen Relevanz für die Sicherung der kritischen Infrastruktur nicht einer rein wettbewerblichen Selbststeuerung überlassen werden. Sowohl die staatlichen Behörden als auch die privaten Unternehmen stützen sich auf Informations- und Kommunikationssysteme. Ausfälle oder anderweitige Beeinträchtigungen dieser Systeme besitzen ein weitreichendes, kaum quantifizierbares Schadenspotenzial. Deutschland muss daher auf eine starke IT-Sicherheitsbranche als wichtige Schlüsselindustrie im eigenen Land zurückgreifen können.

IT-Sicherheit als Politikfeld und Wirtschaftsfaktor

Ordnungspolitisches Handeln im Bereich der IT-Sicherheit sollte die Besonderheiten des Bereichs als Politikfeld und Wirtschaftsfaktor berücksichtigen. Zum einen ist die IT-Sicherheitstechnologie durch einen hohen Komplexitäts- und Innovationsgrad gekennzeichnet; entsprechende Zutrittshemmnisse liegen in der begrenzten Verfügbarkeit von spezialisiertem Expertenwissen sowie im eingeschränkten Zugang zu Ressourcen und Netzwerken. Zum anderen ist die IT-Sicherheit durch ihre enge Verzahnung mit der IT im Allgemeinen ein nicht mehr klar eingrenzbarer Einsatzbereich, der hinsichtlich der Technologie und der Produkte branchenübergreifend Anwendung findet. Aufgrund dieser Ausdehnung und der zunehmenden Bedeutung der IT-Sicherheit für nahezu alle Bereiche des öffentlichen, wirtschaftlichen und privaten Lebens berührt dieses Thema zwangsläufig die Geschäftsbereiche verschiedener Ressorts der Bundesregierung: von der Wirtschaft über die For-

schung und die innere Sicherheit bis zum Verbraucherschutz und den Außenbeziehungen.

Das Marktumfeld für die IT-Sicherheit

Bei der Beurteilung des ordnungspolitischen Handlungsbedarfs für die IT-Sicherheitsbranche sind des Weiteren die Besonderheiten des Marktumfelds in Betracht zu ziehen. Der Markt für IT-Sicherheitsprodukte und -dienstleistungen ist insgesamt weit von einer Situation reinen und perfekten Wettbewerbs entfernt. Der Markt ist gekennzeichnet durch eine dominante Stellung weniger global agierender Anbieter, vor allem amerikanischer Unternehmen wie Symantec, Cisco oder McAfee. Auch zeichnet sich dieser Markt aufgrund seiner Bedeutung für die Sicherheitsinteressen des jeweiligen Landes generell durch erheblichen staatlichen Einfluss aus. Dies zeigt sich zum Beispiel in der Besetzung und Beeinflussung von internationalen Gremien, wie beispielsweise der ISO, ITU, W3C[156] für die Standardisierung von IT-Sicherheit oder der ICANN[157] für die Verwaltung und Entwicklung des Internets. Der staatliche Einfluss kommt auch in der Vielzahl von Vorschriften und Beschränkungen zum Ausdruck, die im Zusammenhang mit Lieferungen von Sicherheitstechnologie an öffentliche Auftragnehmer im In- und Ausland zu beachten sind. So ist zum Beispiel der Zugang zu ausländischen Märkten, vor allem zu Regierungsaufträgen, erschwert und in der Regel von aufwendigen Zertifizierungs- und Zulassungsverfahren abhängig. Schließlich unterliegt der Export von IT-Sicherheitstechnologie in vielen Fällen der Ausfuhrkontrolle. Das Zustandekommen von Auslandsgeschäften ist zudem von guten bilateralen Beziehungen sowie von einer aktiven Unterstützung des Staates u. a. bei der Kontaktvermittlung abhängig.

Der deutsche IT-Sicherheitsmarkt ist gekennzeichnet durch einen hohen Fragmentierungsgrad (vgl. auch Abschnitt 5.1), d. h. einen hohen Anteil kleiner und mittelgroßer Unternehmen (bis etwa 300 Mitarbeiter), die sich weniger auf das IT-Massengeschäft als vielmehr auf die Bereitstellung technologisch hochwertiger IT-Sicherheitstechnologie spezialisiert haben. Zudem haben et-

[156] ISO – International Standards Organization, ITU – International Telecommunications Union, W3C – World Wide Web Consortium

[157] ICANN – International Cooperation for Assigned Names und Numbers

liche deutsche Anbieter einen starken Branchenfokus auf die öffentliche Verwaltung und sind zu einem guten Teil von Regierungsaufträgen abhängig, z. B. D-Trust, GeNUA, Rohde & Schwarz, secunet oder Sirrix. Diese Spezialisierung und die beschränkte Verfügbarkeit von Kapital führt zu einer hohen Vulnerabilität dieser kleinen und mittelgroßen Unternehmen. Geringere Wachstumschancen im In- und Ausland sowie mögliche Übernahmen durch stärkere ausländische Konkurrenten sind die Folge. Diese Schwäche ist auch ein Grund für den geringen Anteil deutscher IT-Sicherheitsanbieter am attraktiven globalen IT-Sicherheitsmarkt, der mit einem geschätzten Wachstum von 13,6% im Jahr ein erhebliches Potenzial aufweist.

Schließlich gilt die IT-Sicherheit als ein Prestige-Feld, welches der Staat im Hinblick auf die internationale Reputation der deutschen Volkswirtschaft und der deutschen Ingenieurskunst nicht unbesetzt lassen kann. Die Herkunftsbezeichnung „Made in Germany" kann sehr glaubwürdig mit IT-Sicherheit in Verbindung gebracht werden und bietet den deutschen Anbietern ein Alleinstellungsmerkmal, welches in Verbindung mit dem außenpolitischen Ansehen Deutschlands die Zuverlässigkeit und Vertrauenswürdigkeit der deutschen IT-Sicherheitstechnologie unterstreicht.

Fazit

Aufbauend auf dieser Sicht werden drei Handlungsziele erkannt, in denen der Staat positive Impulse für eine bessere Wettbewerbsfähigkeit der IT-Sicherheitsbranche setzen kann:

- **Sicherstellung kritischer Kompetenzen** im Markt

  Bei diesem Handlungsziel geht es darum, die kritischen Kompetenzen Deutschlands im Bereich der IT-Sicherheit, insbesondere Wissen, Technologie, Fachkräfte und Infrastruktur, zu sichern und festgestellte Schwächen und Lücken zu beheben.

- **Innovation**

  Unter dem Handlungsziel Innovation werden alle Aspekte und Handlungsempfehlungen zusammengefasst, die die Innovationskraft der deutschen Industrie und der FuE-Landschaft im Bereich der IT-Sicherheit erhöhen. Hierzu zählen eine effiziente Forschungs- und Entwicklungsförderung sowie eine wirkungsvolle Flankierung des Zusammenspiels von

Wirtschaft und Forschung oder der Beteiligung der Industrie an Forschungs- und Entwicklungstätigkeiten.

- **Wachstum**

  Das Handlungsziel Wachstum umfasst unterstützende Maßnahmen zur Erschließung weiterer **Wachstumspotenziale**. Hierunter fallen insbesondere die staatliche Flankierung der Exportförderung sowie der Kooperationen unter den Unternehmen.

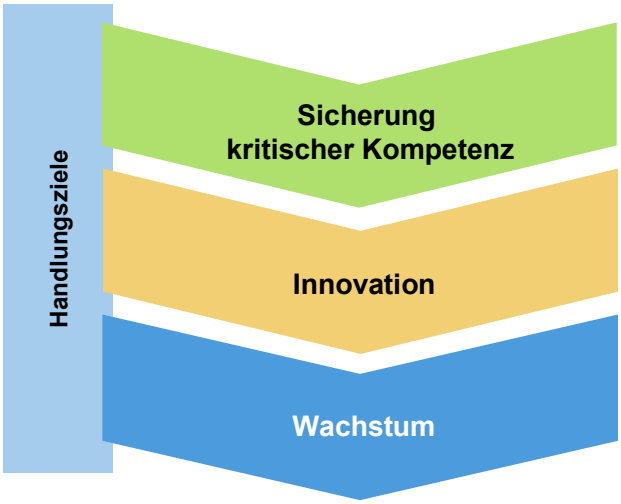


Abbildung 43: Übersicht der Handlungsziele

Im folgenden Kapitel werden diese Handlungsziele näher umschrieben und in konkreten Maßnahmen konkretisiert. Dabei wird der Handlungsspielraum der Wirtschafts-, Industrie- und Handelspolitik in den Vordergrund gestellt.

7.6 Handlungsfelder und Maßnahmen

Die Analyse der Stärken und Schwächen der deutschen IT-Sicherheitsbranche, die zu einem großen Teil auf Beiträgen der befragten Unternehmen und Experten basiert, hat innerhalb der umschriebenen drei Handlungsziele insgesamt elf Handlungsfelder ergeben. Diese Handlungsfelder umfassen alle wesentlichen Aspekte und Politikbereiche, die Einfluss auf die IT-Sicherheit haben. Infolgedessen berühren die genannten Handlungsziele die Zuständigkeitsbereiche verschiedener Ressorts der Bundesregierung, insbesondere der Bundesministerien für Wirtschaft und Technologie (BMWi), des Innern (BMI) und für Bildung und Forschung (BMBF) sowie des Auswärtige Amts (AA). Im Rahmen der vorliegenden Studie werden jedoch die Gestaltungsmöglichkeiten im Geschäftsbereich des BMWi vorrangig betrachtet und. Wo es angebracht erscheint, wird darüber hinaus auf mögliche unterstützende und weiterführende Aktivitäten anderer Teile der Bundesregierung verwiesen.

Abbildung 44: Übersicht der ordnungspolitischen Handlungsfelder

In den folgenden Abschnitten „Sicherung kritischer Kompetenz“ (7.6.1), „Innovation“ (7.6.2) und „Wachstum“ (7.6.3) werden die Handlungsfelder näher erläutert sowie Einzelmaßnahmen zu den Handlungsfeldern vorgestellt, die im unmittelbaren Wirkungskreis des BMWi liegen.

7.6.1 Sicherung kritischer Kompetenz

Für das Handlungsziel „Sicherung kritischer Kompetenz“ haben sich zwei Handlungsfelder ergeben, in denen das BMWi mit Einzelmaßnahmen tätig werden kann. Diese können einen wichtigen Beitrag dazu leisten, die für die IT-Sicherheit kritischen Kompetenzen zu sichern und wichtige Wachstumsimpulse zu geben. Das erste Handlungsfeld befasst sich mit dem Aufbau und der Sicherung der nationalen Expertise (7.6.1.1). Das zweite Handlungsfeld betrifft die Notwendigkeit einer aktiveren Mitgestaltung internationaler IT-Sicherheits-Standards (7.6.1.2). Es haben sich darüber hinaus im Rahmen dieser Studie auch Handlungsoptionen im Geschäftsbereich anderer Ressorts der Bundesregierung ergeben, um aufgezeigte Schwächen im Bereich der Sicherung kritischer Kompetenz zu beheben. Hierzu gehören die Schaffung einer „vertrauensvollen Werkbank“ in Deutschland und die Schließung von Lücken in der Wertschöpfungskette für IT-Sicherheit. Des Weiteren gehört hierzu die Möglichkeit, den Einsatz von zertifizierter IT-Sicherheitstechnologie auf den Systemen der Bundesregierung und des ihr nachgeordneten Bereichs zu forcieren. Dadurch könnte der Staat Einfluss auf das Angebot an zertifizierter IT-Sicherheitstechnologie nehmen – vorausgesetzt, die Unternehmen können mit einer Zertifizierung ihrer Produkte innerhalb der in der IT-Branche üblichen kurzen Produktentwicklungszyklen rechnen.

7.6.1.1 Aufbau und Sicherung der nationalen Expertise

In diesem Handlungsfeld geht es darum, die bestehende Kompetenz in Deutschland zum Thema IT-Sicherheit zu sichern und dort, wo Lücken erkannt werden, den Aufbau der fehlenden Expertise in Angriff zu nehmen. Zu diesem Zweck kann es sinnvoll sein, einen Kompetenz-Monitor aufzubauen und zu pflegen, der eine gezielte Förderung und Unterstützung bestehender sowie den Aufbau fehlender kritischer IT-Sicherheitskompetenzen in Deutschland, zum Beispiel in Hochschulen und weiterführenden Schulen, ermöglicht.

Für den Geschäftsbereich des BMWi ergeben sich eine Reihe von Einzelmaßnahmen, die jede für sich einen wichtigen Beitrag dazu leisten können, kritische Kompetenzen in der IT-Sicherheit für Deutschland zu sichern:

- Erstellung und regelmäßige Pflege eines deutschen Branchenregisters IT-Sicherheit mit allen Firmen der IT-Sicherheitsbranche in Deutschland: Die kann ggf. auf der Basis des Branchenbuchs IT-Sicherheit

(www.branchenbuch-itsicherheit.de) und unter Beteiligung einer neu ausgerichteten ITSMIG e.V. (vgl. auch 7.6.3.1) erfolgen. Die IT-Sicherheitsbranche ist aufgrund ihrer von KMU geprägten Struktur in der Regel nicht von der Kartell-, der Wertpapier- oder der Finanzdienstaufsicht erfasst, die das BMWi mit entscheidenden Informationen zu geplanten Firmenübernahmen versorgen. Daher benötigt das BMWi ein Instrument für die wirksame Beobachtung des Marktgeschehens im IT-Sicherheitsbereich. Das Branchenregister IT-Sicherheit soll das BMWi durch folgende Aspekte unterstützen:

  - vollständiger und aktueller Überblick über die IT-Sicherheitsanbieter in Deutschland,
  - Möglichkeit einer pro-aktiven Betreuung der deutschen IT-Sicherheitsanbieter,
  - Unterstützung bei der Prüfung evtleventueller Übernahmen durch ausländische Investoren nach § 7 AWG i. V. m. §§ 52 und 53 AWV.[158]

- Evaluierung der bisherigen Anwendungspraxis zu § 7 AWG i. V. m. §§ 52 und 53 AWV. Diese sollte im Hinblick auf die KMU-Struktur der deutschen IT-Sicherheitsanbieter erfolgen. Auf dieser Basis kann ein Handlungsrahmen „Zukunftsbranche IT-Sicherheit" zur pro-aktiven Unterstützung der im Branchenregister IT-Sicherheit aufgelisteten Firmen und zur Früherkennung möglicher Genehmigungsfälle erarbeitet werden.
- Evaluierung des bestehenden Aus- und Weiterbildungsangebots der Wirtschaft und der öffentlichen Verwaltung mit Blick auf:
  - Ausbildungsberufe im Bereich IT-Sicherheit, z. B. „IT-Sicherheitstechniker",
  - Sensibilisierung der Mitarbeiter in Unternehmen und Verwaltung,
  - Fachwissen für IT-Sicherheitsbeauftragte in Unternehmen und Verwaltung,
  - Ergänzung um Lehrgänge oder Ausbildungsinhalte zum Thema „IT-Sicherheit".

[158] Regelungen zum Genehmigungsverfahren von Übernahmen deutscher Unternehmen durch nicht-deutsche (§ 52AWV) bzw. nicht EU ansässige (§ 53 AWV) Investoren.

- Aufbau von Austauschprogrammen im Bereich der IT-Sicherheit: Dies betrifft den Austausch zum einen zwischen Wirtschaft und Regierung/Verwaltung und zum anderen zwischen Experten der öffentlichen Verwaltung und ausländischen IT-Sicherheitsstellen (Zertifizierungsstellen, Stellen für den Schutz kritischer Telekommunikationsinfrastruktur) zur Förderung des Wissenstransfers mit ausgewählten Ländern.
- Unterstützung des „Deutschen IT-Sicherheitspreises" der Horst-Görtz-Stiftung[159]: Der Deutsche IT-Sicherheitspreis wurde bereits zweimal vergeben (2006 und 2008). Die Horst-Görtz-Stiftung widmet sich der Förderung von Wissenschaft und Technik in Forschung und Lehre, mit einem besonderen Schwerpunkt auf der Informationssicherheit. Es könnte sinnvoll sein, diesen Preis zum nationalen IT-Sicherheitspreis auszubauen und dabei eine Reihe von Preiskategorien festzulegen, z. B. „bester Nachwuchs", „beste Verschlüsselung", „größte entdeckte Sicherheitslücke", „sicherstes Unternehmen", „bestes neuartiges Geschäftsmodell".
- Wirtschaftspolitische Begleitung der Schließung der Lücken in der Wertschöpfungskette für eine „vertrauensvolle Werkbank" in Deutschland. Potenzielle Einzelmaßnahmen sind z. B. der Aufbau nationaler Anbieter, die Förderung von Kooperationen, strategische Partnerschaften innerhalb der EU (ggf. unter Einbeziehung der europäischen Agentur für Netz- und Informationssicherheit [ENISA] und der europäischen Verteidigungsagentur [EDA]).

7.6.1.2 Aktivere Mitgestaltung internationaler Standards der IT-Sicherheit

In diesem Handlungsfeld geht es darum, über eine starke Beteiligung und Einflussnahme bei der Erarbeitung von internationalen Standards deutsche IT-Sicherheitstechnologie international zu verbreiten und somit die Stellung und die Marktchancen der deutschen IT-Sicherheitsbranche positiv zu beeinflussen. Für dieses Handlungsfeld wurden die folgenden Einzelmaßnahmen im Geschäftsbereich des BMWi identifiziert:

- Evaluierung der derzeitigen Arbeit beim DIN und der deutschen Beteiligung an internationalen Standardsetzungen zum Thema IT-Sicherheit. Durch den direkten Vergleich mit der Beteiligung der wichtigsten Auslandsmärkte in der internationalen Standardisierung sollten Optimie-

[159] Horst Görtz ist der Gründer der Utimaco Software GmbH, später Utimaco Safeware AG

rungsmöglichkeiten für die Präsenz und Einflussnahme Deutschlands erarbeitet werden. Dabei sollten die Auswirkungen der Beteiligung auf die Marktpräsenz und die Wachstumschancen untersucht und wesentliche „best practices" abgeleitet werden.

- Erstellung eines Aktionsplans zur Verbesserung der deutschen Beteiligung (Wirtschaft und Regierung) in wesentlichen europäischen und internationalen Standardgremien zum Thema IT-Sicherheit (ETSI, CEN, CENELEC, IEC, ITU, W3C, OASIS, ISO, GS1, EPC Global usw.) auf der Basis der Evaluierung und der Vergleichstudie, und zwar durch folgende Maßnahmen:
  - Durchführung von Workshops beim „Branchenforum IT-Sicherheit" (vgl. 7.6.3.2) zur Sensibilisierung für die Bedeutung dieses Themas und zur Vorstellung von „best practices" aus der deutschen Wirtschaft,
  - Koordinierung der deutschen Beteiligung in internationalen Gremien durch Erarbeitung von deutschen Beiträgen bzw. Normentwürfen bei den entsprechenden Spiegelausschüssen bzw. Arbeitskreisen beim DIN, ggf. Einrichtung weiterer Spiegelausschüsse bzw. Arbeitskreise, wo diese noch fehlen,
  - Sicherstellung der deutschen Teilnahme an den internationalen Gremiensitzungen, zumindest durch die Vorsitzenden der relevanten DIN-Arbeitskreise.

7.6.2 Innovation

Zur Stärkung der Innovationskraft wurden fünf Handlungsfelder mit verschiedenen Einzelmaßnahmen herausgearbeitet. Zunächst wird das Handlungsfeld Fokussierung und Konzentration der FuE-Förderung (7.6.2.1) beschrieben. Danach werden Maßnahmen zur Verbesserung des Schutzes geistigen Eigentums (7.6.2.2) sowie zum Ausbau der Kooperationen zwischen Industrie und Forschung (7.6.2.3) vorgestellt. Anschließend wird auf die Vorbildfunktion des Staates beim Einsatz innovativer IT-Sicherheitsprodukte (7.6.2.4) eingegangen, bevor mit Vorgaben und Anreizen für Unternehmen zum Einsatz von IT-Sicherheit (7.6.2.5) dieses Kapitel abgeschlossen wird.

7.6.2.1 Fokussierung und Konzentration der FuE-Förderung

Bei der Fokussierung und Konzentration der FuE-Förderung steht die Exzellenzförderung im Mittelpunkt, also die Bildung von IT-Sicherheitsclustern

und die Forcierung der anwendungsorientierten Forschung mit dem Ziel, Deutschland als Forschungsstandort für die IT-Sicherheit an die internationale Spitze zu führen. Der Schwerpunkt dieses Handlungsfelds liegt im Geschäftsbereich des BMBF, doch auch das BMWi kann mit den folgenden Einzelmaßnahmen wichtige Impulse setzen:

- Auflegen eines Pilotprogramms (zeitlich und finanziell eng begrenzt) mit dem Ziel, Erfahrungen mit der Förderung von Risikoforschung[160] über IT-Sicherheit mit einer Förderquote von bis zu 100% zu gewinnen.
- Anschließende Auswertung der Erkenntnisse und Erfahrungen des Pilotprogramms für die Entscheidung über eine mögliche Initiative zur Ergänzung der EU-Beihilferichtlinien für Forschung und Entwicklung, und zwar im Sinne einer Förderung von Risikoforschung mit einer Förderquote von bis zu 100%.

7.6.2.2 Verbesserung des Schutzes geistigen Eigentums

Der Schutz des geistigen Eigentums ist ein wichtiger Bereich für die Unternehmen aber auch ein wichtiges Politik- und Regelungsfeld, insbesondere um technologiegetriebene Industrien wie die IT-Sicherheit wirksam vor ungewolltem Wissensabfluss und Technologietransfer zu bewahren. Dieses Handlungsfeld umfasst eine Reihe von Einzelmaßnahmen, die sich einerseits mit der IT-Sicherheit als schützenswerter Technologie befassen und andererseits mit der IT-Sicherheitstechnologie als wirksamem Mittel zum Schutz des geistigen Eigentums. Zu der ersten Kategorie gehören u. a. die Regierungsabkommen über die gegenseitige Anerkennung von IT-Sicherheitszertifikaten, die alle wichtigen Zielmärkte für die deutsche IT-Sicherheitsbranche abdecken sollten. Im direkten Wirkungskreis des BMWi ergeben sich folgende Einzelmaßnahmen:

- Durchführung einer empirischen Vergleichsstudie auf der Basis von Primärerhebungen und -analysen zur Feststellung von Einfuhr- und Marktzugangsbeschränkungen für deutsche IT-Sicherheitstechnologie in wichtigen Zielmärkten:
  - Anforderungen an die Einhaltung technischer Standards,

[160] Forschung mit höchst ungewissenem Ausgang und hohem finanziellen Risiko

  - Anforderungen an die Vorlage von vertrauenswürdigen Geschäftspapieren und technischen Unterlagen zur Erlangung von für die Einfuhr notwendigen Bescheinigungen und Zertifikaten,
  - Schutz des geistigen Eigentums.

- Evaluierung der bestehenden Informationsreihen und -kampagnen von Bund und Wirtschaft zum Themenfeld „Schutz des geistigen Eigentums" im Hinblick auf die Bedeutung der IT-Sicherheit für den Schutz des geistigen Eigentums. Eine Durchführung neuer Informationsreihen erscheint zu folgenden Themen sinnvoll:
  - Entwicklung und Einsatz von IT-Sicherheitstechnologie für den Schutz von geistigem Eigentum,
  - Einfluss des Staates und nationaler Interessen beim Schutz des geistigen Eigentums von Hochsicherheitstechnologie,
  - Schutz von geistigem Eigentum bei Forschungskooperationen.

7.6.2.3 Ausbau der Kooperationen zwischen Industrie und Forschung

Die Kooperation zwischen Industrie und Forschung wurde von vielen der im Rahmen dieser Studie befragten Unternehmen als verbesserungswürdig eingestuft. In diesem Handlungsfeld sollten daher mit einer Reihe von Einzelmaßnahmen Impulse gesetzt werden mit dem Ziel, die Bereitschaft und das Klima für Kooperationen zwischen Industrie und Forschung zu verbessern. (Angesichts der im Vergleich zum Ausland – z. B. den USA oder Frankreich – generell gering ausgeprägten Kooperationsbereitschaft innerhalb der deutschen Wirtschaft wird dieses Ziel allerdings wohl eher langfristig anzusetzen sein.) Ein wichtiger Aspekt in diesem Handlungsfeld wird es ferner sein, die zuständigen öffentlichen Stellen dahingehend zu sensibilisieren, dass sie steuerfinanzierte Forschungseinrichtungen bzw. die Hochschulen nicht als Anbieter in den direkten Wettbewerb mit der Industrie eintreten lassen, z. B. bei Ausschreibungen der öffentlichen Hand. Auch im Geschäftsbereich des BMWi finden sich Ansätze, diese Konkurrenzsituationen aufzulösen, u. a. durch verstärkte Förderung von Ausgründungen.

Darüber hinaus beinhalten die folgenden Maßnahmen im Geschäftsbereich des BMWi weitere wichtige Ansätze zur Förderung der Kooperation zwischen Industrie und Forschung:

- Förderung von Ausgründungen (Spin-offs) aus Hochschulen und Forschungseinrichtungen im Bereich der IT-Sicherheit,
- Aufbau eines Gründernetzwerks „IT-Sicherheit" mit Webportal und Diskussionsforen unter der Schirmherrschaft des BMWi,
- Einrichtung eines Gründerstipendiums „IT-Sicherheit" im Rahmen des EXIST-Gründerstipendium-Programms des BMWi,
- Auflage eines Gründerprogramms „IT-Sicherheit" bei der KfW-Mittelstandsbank,
- Förderung der Übernahme von Gründerpatenschaften „IT-Sicherheit" durch Unternehmen, unter Einbindung des vorgeschlagenen „Branchenforums IT-Sicherheit" (vgl. 7.6.3.2),
- Durchführung eines Förderwettbewerbs „Kooperation in der IT-Sicherheit" zur Verbesserung der Zusammenarbeit zwischen Wirtschaft und Forschung mit regelmäßig wechselnden Schwerpunktthemen (z. B. beste „Time-to-market"-Kooperation). Der Förderwettbewerb sollte vom BMWi unter Einbindung des BMBF und der Verbände der IT-Sicherheitsindustrie (TeleTrust, ITSMIG e.V., BitKOM) organisiert und ausgetragen werden.

7.6.2.4 Vorbildfunktion des Staates bei der Anwendung innovativer IT-Sicherheitsprodukte

In diesem Handlungsfeld wird die Vorbildfunktion des Staates aktiviert. Durch konsequenten Einsatz innovativer IT-Sicherheitsprodukte auf den IT-Systemen des Staates kann der Staat die Wirtschaft und die privaten Haushalte dazu anleiten, diesem Beispiel zu folgen. Dabei kann die Umsetzung durch das Vorgeben von Mindeststandards im öffentlichen Bereich erfolgen oder durch verstärkte Verwendung von Ergebnissen der IT-Sicherheitsforschung in Pilotanwendungen. Die ausstrahlende Wirkung auf die Wirtschaft und die Haushalte hängt dabei von einer wirksamen Außendarstellung ab, die die Auswirkungen auf die Innovation, das Wachstum und den verbesserten Schutz der kritischen Infrastruktur IKT herausstellt. Dieses Handlungsfeld zielt überwiegend auf die öffentliche Verwaltung ab und liegt somit im Geschäftsbereich des BMI. Gleichwohl kann auch das BMWi mit der folgenden Einzelmaßnahme einen wichtigen Beitrag zu diesem Handlungsfeld leisten:

- Definition neuer Leuchtturmprojekte für den Einsatz von IT-Sicherheit bzw. sicherer IT in Zusammenarbeit mit der Wirtschaft. Dies ist vor allem in besonders anfälligen und sensiblen Bereichen wie Banken (Onlinebanking, Geldautomaten, Debit- und Kreditkarten usw.), Gesundheit, elektronischer Handel und soziale Netzwerke relevant.

7.6.2.5 Vorgaben und Anreize für Unternehmen zum Einsatz von IT-Sicherheit

Neben Vorgaben für Unternehmen zum Einsatz von IT-Sicherheit, z. B. im Zusammenhang mit E-Government-Anwendungen oder elektronischem Geschäftsverkehr mit der Verwaltung, sollte die Regierung vornehmlich auf Anreize setzen, Unternehmen zum Einsatz von IT-Sicherheit zu bewegen. Hierzu zählt auch, Unternehmen die Ergebnisse aus der IT-Sicherheitsforschung als kostenlose Betaversionen über ein zentrales Webportal zugänglich zu machen.

Im Geschäftsbereich des BMWi gibt es ebenfalls Möglichkeiten, wichtige Anreize zum Einsatz von IT-Sicherheit zu setzen. Hierzu gehören u. a. rechtliche und finanzielle Anreize, wobei bei Letzteren mit Blick auf die angespannte Haushaltslage wohl nur wenig Aussicht auf Umsetzung durch das BMWi bzw. das BMF besteht:

- Schaffung rechtlicher und finanzieller Anreize für den Einsatz von „sicherer“ IT, d. h. IT mit Sicherheitszertifikat, und der Sicherheitszertifizierung von Unternehmen nach ISO 27001, z. B. durch:
  - Verkürzung des steuerlichen Abschreibungszeitraums gegenüber herkömmlicher IKT,
  - Mehrwertsteuerbefreiung (bzw. reduzierter Satz) für IT-Sicherheitsprodukte und -dienstleistungen,
  - Berücksichtigung einer IT-Sicherheitszertifizierung beim Kredit-Rating oder beim Versicherungsschutz,
  - Verschärfung der Kontrollanforderungen: Der Einsatz herkömmlicher IKT in gefährdeten Unternehmensbereichen und das Fehlen einer IKT-Sicherheitsstrategie und -zertifizierung in Unternehmen

könnte als fahrlässige Aufsichtspflichtverletzung gelten und somit unter die Regelung des § 130 OWiG[161] fallen.

- Förderung des elektronischen Geschäftsverkehrs und der Verbreitung der digitalen Signatur in der Wirtschaft, insbesondere bei den KMU, durch Vereinfachung der elektronischen Rechnungsstellung im Umsatzsteuerrecht:
  - Unterstützung der Bundesregierung für den Richtlinienentwurf der EU-Kommission zur Änderung der Anforderungen an die elektronische Signatur bei der elektronischen Rechnungsstellung[162] und Vorbereitung der zügigen Umsetzung der Richtlinie in nationales Recht nach ihrem Inkrafttreten.

7.6.3 Wachstum

Im Handlungsfeld "Wachstum" wurden vier wesentliche Handlungsfelder herausgearbeitet, die sich auf die Wachstums- und Exportchancen der deutschen IT-Sicherheitsbranche auswirken. Neben einer verstärkten Unterstützung und Erleichterung des Exports (7.6.3.1), der Zusammenarbeit mit und innerhalb der Wirtschaft (7.6.3.2) und einer wirksameren Aufklärungsarbeit der Regierung zu IT-Sicherheit (7.6.3.3) kommt insbesondere den Erleichterungen für die Kapitalbeschaffung (7.6.3.4) eine große Bedeutung zu.

7.6.3.1 Unterstützung und Erleichterung des Exports

Die Unterstützung und Erleichterung des Exports ist ein wesentliches Handlungsfeld, um für die deutsche IT-Sicherheitsbranche wichtige Wachstumspotenziale zu erschließen. Insbesondere ein stärkeres staatliches Engagement für die KMU der deutschen IT-Sicherheitsbranche bei der Kontaktvermittlung, Informationsbeschaffung und Geschäftsanbahnung ist für den sensiblen Bereich der IT-Sicherheit von großer Bedeutung. Es sollten daher Gespräche mit

---

[161] § 130 OWiG regelt, daß der Inhaber eines Unternehmens ordnungswidrig handelt, wenn in seinem Unternehmen durch seine fahrlässige oder vorsätzliche Aufsichtspflichtverletzung eine Straftat (z. B. Verletzung des Datenschutzes) geschieht. Der Unternehmer kann mit einer Geldbuße von bis zu 1 Mio. Euro belegt werden.

[162] Siehe COM(2009) 21 final

dem Auswärtigen Amt (AA) über ein Dienstleistungsangebot der Botschaften in wichtigen Zielmärkten für die deutschen IT-Sicherheitsanbieter stattfinden.

Darüber hinaus bieten sich folgende Maßnahmen im Geschäftsbereich des BMWi zur Umsetzung dieses Handlungsfeldes an:

- Vereinbarung von Zielen für eine ressortübergreifende Exportunterstützung für die IT-Sicherheitsbranche, insbesondere auf Bundesebene (BMWi, AA, BMI, BMZ), z. B.:
  - Erhöhung des Anteils der IT-Sicherheitsausfuhren an der Gesamtausfuhr von Gütern und Dienstleistungen,
  - Positionierung der IT-Sicherheitstechnologie „Made in Germany" als „vertrauenswürdige Spitzentechnologie" in den wichtigen Zielmärkten Südostasien, Osteuropa, Mittlerer Osten und Nordamerika.
- Analyse und Optimierung der Zusammenarbeit von BAFA, BMWi und AA beim Verfahren der Exportkontrolle für IT-Sicherheitstechnologie, zum Beispiel durch Festlegung einer Bearbeitungsfrist für Anträge auf Ausfuhrgenehmigung (wie in der Dual-Use-VO der EU vorgesehen) mit den folgenden Kriterien:
  - Maximaldauer von 20 Tage für die Erteilung der Ausfuhrgenehmigung bzw. eines Zwischenbescheids mit Angabe der voraussichtlichen Dauer,
  - Ziel einer durchschnittlichen Bearbeitungszeit von fünf Tagen (z. B. berechnet über einen 6-Monats-Zeitraum),
  - halbjährliche Veröffentlichung der Zielerreichung.
- Neuausrichtung und umfassendere Ausgestaltung der ITSMIG e.V. als zentrale Anlaufstelle der deutschen IT-Sicherheitsbranche, z. B. durch:
  - bessere Abstimmung der Regierungsunterstützung,
  - bessere finanzielle Förderung, ggf. durch eine neue Gesellschaftsform und eine Beteiligung des Staates,
  - Übernahme der Geschäftsstelle durch das BMWi oder anderweitige Bereitstellung bzw. Abordnung von Personal zur Unterstützung,
  - Einbindung des Auswärtigen Amts und der Auslandsvertretungen,

  - Ausdehnung des geographischen Betätigungsfeldes auf Südostasien, Osteuropa und den Mittleren Osten,
  - PR- und Marketingunterstützung für Mitglieder, z. B. auf Auslandsmessen und Delegationsreisen.

- Erleichterung der Teilnahme von KMU der IT-Sicherheitsbranche an Delegationsreisen der Bundesregierung in wichtige Zielmärkte, z. B.:
  - Delegationsreisen, die speziell auf IT und IT-Sicherheit ausgerichtet sind,
  - Etablierung einer Anlaufstelle für KMU bei einer neuausgerichteten ITSMIG e.V.,
  - regelmäßige Teilnahme der ITSMIG e.V. bei Delegationsreisen in die wichtigsten Zielmärkte als Vertreter der deutschen IT-Sicherheitsbranche.
- Einrichtung einer zentralen Kontaktstelle mit Callcenter und internem Know-how bei der GTAI unter Einbindung des Informationsportals XPOS und der Außenhandelskammern für die Außenwirtschaftsförderung der IT-Sicherheitsbranche und für die Beratung über potenzielle ausländische Übernahmeobjekte im IT-Sicherheitsbereich in Zielmärkten.

7.6.3.2 Intensivierung der Zusammenarbeit mit und innerhalb der Wirtschaft

Die Zusammenarbeit der Regierung mit der Privatwirtschaft, aber vor allem der Unternehmen untereinander wurde als eine markante Schwäche der deutschen IT-Sicherheitsbranche herausgestellt. Dieses Handlungsfeld zielt daher darauf ab, über regelmäßige Kommunikation und Begegnungen die Kooperationsbereitschaft der Beteiligten zu fördern. Im Einzelnen werden folgende Maßnahmen im Geschäftsbereich des BMWi vorgeschlagen:

- Einrichtung eines „Branchenforums IT-Sicherheit“ beim BMWi unter gemeinsamer Leitung des BMWi und eines Vertreters der teilnehmenden Unternehmen mit dem Ziel, die Kommunikation und Kooperation der IT-Sicherheitsbranche untereinander und mit der Regierung nachhaltig zu fördern und die Exportchancen zu verbessern, u. a. durch:
  - Diskussionsrunden zu relevanten Markttrends und Entwicklungen auf den Auslandsmärkten,

  - Beteiligung des Forums bei der Erarbeitung und Aktualisierung des nachstehend skizzierten Aktionsplans Auslandsmessen,
  - Durchführung von Workshops in Zusammenarbeit mit der „neuen" ITSMIG e.V. (vgl. 7.6.3.1) zu Themen wie: deutsche Beteiligung bei der internationalen Standardisierung, Wachstumsstrategien, Erschließung von Auslandsmärkten, Vertriebs- und Marketingkompetenz und -konzepte für den Export,
  - Übernahme von Gründerpatenschaften in der IT-Sicherheit,
  - Erarbeitung gemeinsamer Eckpunkte zur Positionierung des Standorts Deutschlands mit Blick auf die Handlungsziele Wachstum, Innovation und Sicherung kritischer Kompetenz.

- Ausarbeitung eines Aktionsplans zum Ausbau des Messestandorts Deutschland für die IT-Sicherheit, z. B. mit den folgenden Eckpunkten:
  - Weiterentwicklung der IT-Sicherheitsmesse IT-SA in Nürnberg zur wichtigsten internationalen Messe für IT-Sicherheit (z. B. Eröffnung durch Minister),
  - Koordinierung der Regierungsbeteiligung bei anderen Messen wie CeBIT, PITS (Public IT Security), „Security" in Essen, Sicherheit Expo München.
- Erstellung eines Aktionsplans „Auslandsmessen IT-Sicherheit" (z. B. RSA, GITEX) zur Verbesserung der deutschen Präsenz, u. a. durch:
  - Erleichterung der Teilnahme von KMU (ggf. durch ITSMIG e.V.),
  - Einbeziehung der IT-Sicherheitsforschung,
  - gemeinsame Schirmherrschaft von BMWi, BMI und BMBF sowie Ministerbesuch.
- systematische Positionierung des Themas IT-Sicherheit bei einschlägigen Konferenzen und Veranstaltungen der Bundesregierung, z. B. „Deutscher Außenwirtschaftstag", IT-Gipfel, START-Messe u. Ä.

7.6.3.3 Aufklärungsarbeit der Regierung zur IT-Sicherheit

Wichtige Nachfrageimpulse für die IT-Sicherheit können ebenfalls gesetzt werden durch eine wirksame und zielgruppenorientierte Aufklärungsarbeit zum Thema IT-Sicherheit. Dieses Handlungsfeld enthält zwei konkrete Maß-

nahmen, wie das BMWi eine Verbesserung der Aufklärungsarbeit erzielen kann:

- Evaluierung der bestehenden Aufklärungs- und Informationskampagnen der Regierung (insbesondere BMI, BMBF, BMWi und BSI) zur IT-Sicherheit und zu den anwendungsbezogenen Programmen wie der Gesundheitskarte, der digitalen Signatur oder dem elektronischen Personalausweis, und zwar im Hinblick auf Zielgruppen, Verbreitungskanäle, eingesetzte Medien und Aktualität.
- Erarbeitung einer hochrangigen Medienkampagne zur IT-Sicherheit auf der Basis der Evaluierung: Diese sollte gemeinsam mit der Wirtschaft und unter Beteiligung von Ministern, Unternehmensführern und anderen Identifikationspersonen des öffentlichen Lebens stattfinden. Die Kampagne sollte die einzelnen Zielgruppen spezifisch adressieren und folgende Zielsetzungen verfolgen:
    - Erhöhung des Bewusstseins in der Wirtschaft und in der Bevölkerung für die Notwendigkeit der IT-Sicherheitsvorsorge (z. B. durch zielgruppenorientierte, einprägsame Slogans wie „Ich schütze mich“, „Safer Web“, „Ich surfe nicht ohne …“),
    - Verbesserung des Bekanntheitsgrads bestehender Aktivitäten und Initiativen, wie z. B. “Netzwerk für den elektronischen Geschäftsverkehr (NEG)“.

7.6.3.4 Erleichterungen für die Kapitalbeschaffung

Die deutsche IT-Sicherheitsbranche mit ihren überwiegend kleinen und mittleren Unternehmen leidet sehr stark unter der Schwäche des deutschen Finanz- und Kapitalmarkts, diese Branche mit dem notwendigen Kapital auszustatten, um in diesem hochinnovativen Feld Wachstumspotenziale im In- und Ausland zu nutzen. Dieses Handlungsfeld umfasst eine Reihe von Maßnahmen, die es der deutschen IT-Sicherheitsindustrie erleichtern, sich mit Kapital für ihre Wachstumspläne auszustatten:

- Evaluierung der bestehenden Finanzierungsmöglichkeiten der Bundesregierung und der Länder (z. B. KfW-Mittelstandsbank, NRW-BANK): Fokus sollten die Förderungsmöglichkeiten für Unternehmen der IT-Sicherheitsbranche in den Phasen „Seed“, „Start-up“ und „Expansion“ sein. Falls erforderlich, sollten Optimierungs- und Verbesserungsvor-

schläge erarbeitet werden (einschließlich Monitoring-Möglichkeiten zur Überprüfung der Wirksamkeit und Zielerreichung).

- Vergleich der steuerrechtlichen Behandlung von Risikokapitalinvestitionen in den USA, Israel, dem Vereinigten Königreich und Frankreich mit den in Deutschland geltenden Regelungen (vgl. das MoRaKG[163]). Falls nötig, sollte unter Ausschöpfung der EU-Risikokapitalleitlinien eine Angleichung der Bedingungen erfolgen mit dem Ziel, die Risikobereitschaft privater Investoren und Investment-Fonds zu erhöhen und dadurch die Kapitalausstattung der deutschen IT-Sicherheitsbranche zu verbessern (vgl. auch „Sicherung der vertrauensvollen Werkbank"). Zu den zu vergleichenden Bedingungen zählen z. B.:
  - Abschreibungsbedingungen,
  - Regelungen zum Verlustvortrag,
  - Steuerbefreiungen, z. B. von Veräußerungsgewinnen bei Privatinvestoren (sog. „business angels").
- Einrichtung einer gemeinsamen Stiftung von Bund und Wirtschaft oder eines gemeinsamen Risiko-Investmentfonds „IT-Sicherheit" zur Unterstützung von Risikoforschung für mehr Innovation in der IT-Sicherheit (vgl. auch die Ausführungen zum Handlungsfeld „Innovation").

[163] Gesetz zur Modernisierung der Rahmenbedingungen für Kapitalbeteiligungen (BGBl. I 2008 Nr. 36, S. 1672)

7.7 Priorisierung und möglicher Zeitrahmen der Handlungsoptionen

In diesem Abschnitt wird eine Bewertung der im vorherigen Abschnitt 7.6 näher dargestellten Einzelmaßnahmen anhand von drei Dimensionen vorgenommen: Auswirkungen, Realisierbarkeit und Zeit. Das Ergebnis der Bewertung wird in einer Matrix zusammengeführt, aus der über eine Clusterbildung eine Priorisierung für die Umsetzung abgeleitet wird (Abschnitt 7.7.1). Hierauf folgt eine Bewertung der Auswirkungen der ermittelten Cluster (Gruppen) auf die übergeordneten Handlungsziele „Sicherung", „Innovation" und „Wachstum" (Abschnitt 7.7.2). Abschließend wird ein zeitlicher Rahmen vorgestellt, innerhalb dessen die Umsetzung der Maßnahmen in den nach Priorität geordneten Gruppen erfolgen könnte. Hierbei wird auch eine Auswahl an wichtigen Meilensteinen skizziert (Abschnitt 7.7.3).

7.7.1 Priorisierung

Aus den in Abschnitt 7.5 vorgestellten elf Handlungsfeldern wurden insgesamt 36 Einzelmaßnahmen abgeleitet (vgl. Abschnitt 7.6).

Die Ausprägungen für die Bewertungskriterien Auswirkungen und Realisierbarkeit werden in fünf Stufen von „Sehr hoch" bis „Keine" eingeteilt und mittels Harvey-Balls dargestellt. Die Ausprägungen bei der Kategorie Auswirkungen beziehen sich dabei auf die weiterführende Nutzung und effektive Anwendung der von der jeweiligen Maßnahme betroffenen bzw. eingesetzten Instrumente.

Abbildung 45: Übersicht über die fünf möglichen Ausprägungen mittels Harvey-Balls

Das Spektrum der Ausprägungen wird anhand der stärksten und schwächsten Ausprägung kurz vorgestellt:

- Die Ausprägung **„Sehr hoch"** (bzw. voller Harvey-Ball) bedeutet mit Blick auf das angestrebte Ziel eine sehr hohe Wirksamkeit, wobei die Bewertung der Auswirkungen auf prägnanten Parametern aus dem Bereich der einzelnen Handlungsziele basiert, z. B.

- „Wachstum": steigende Ausfuhren, steigende Binnennachfrage nach IT-Sicherheitsprodukten und -dienstleistungen
- „Innovation": größere Zahl der Kooperationen zwischen Wirtschaft und Forschung, steigende Zahl der Ausgründungen bzw. Existenzgründungen im Bereich der IT-Sicherheit
- „Sicherung": größere Beteiligung in internationalen Standardisierungsgremien, sinkende Zahl der Marktaustritte und Firmenübernahmen im Bereich der IT-Sicherheit.

Eine hohe Realisierbarkeit bedeutet dabei, dass die jeweilige Maßnahme aus finanzieller und organisatorischer Sicht sehr leicht umzusetzen ist und somit eine schnelle Wirkung entfalten kann.

- Die Ausprägung **„Keine"** (bzw. leerer Harvey-Ball) bezeichnet eine nicht spürbare und nicht messbare Auswirkung der Maßnahme auf die Handlungsziele. Mit Blick auf die Realisierbarkeit bedeutet diese Ausprägung einen nicht vertretbaren Aufwand in finanzieller, personeller und organisatorischer Hinsicht bei der Umsetzung dieser Maßnahme.

Mit Blick auf die Zeiträume für die Umsetzung der Maßnahmen wird eine Dreiteilung vorgenommen. Dabei wird von dem Zeitpunkt an gerechnet, zu dem diese Studie und damit die hierin enthaltenen Handlungsempfehlungen vom BMWi offiziell verabschiedet werden. Folgende Ausprägungen für die Bewertung des zeitlichen Aufwandes werden verwendet:

- **KF** steht für *kurzfristig* und bedeutet, dass eine Umsetzung der Maßnahme innerhalb von sechs Monaten möglich erscheint.
- **MF** steht für *mittelfristig* und besagt, dass die Umsetzung nach zwölf Monaten abgeschlossen sein kann und dass es ggf. einen Vorlauf von bis zu sechs Monaten geben kann.
- **LF** bedeutet *langfristig* und setzt für die Umsetzung einen Zeitraum von mindestens zwölf Monaten, höchstens jedoch 36 Monaten an. Das Limit von 36 Monaten hat sich aus der Überlegung ergeben, die Maßnahmen innerhalb der laufenden 17. Legislaturperiode umzusetzen.

Die folgende Tabelle gibt einen Überblick über alle 36 Einzelmaßnahmen mit ihren Einzelbewertungen, farblich geordnet nach den Handlungszielen („Sicherung" = grün, „Innovation" = gelb und „Wachstum" = blau).

Tabelle 17: Übersicht über die 36 Einzelmaßnahmen mit ihren Bewertungen[164]

#	Maßnahmenkatalog	Auswir-kungen	Realisier-barkeit	Zeit-rahmen
1.1	Branchenregister IT-Sicherheit	◕	◕	KF
1.2	Anwendungspraxis AWG	◕	◑	MF
1.3	Aus- und Weiterbildungsangebot	◕	◑	MF
1.4	Experten-Austauschprogramm IT-Sicherheit	◑	◑	MF
1.5	Deutscher IT-Sicherheitspreis	◑	●	KF
1.6	Wertschöpfungskette	◕	◔	MF
2.1	DIN-Arbeit IT-Sicherheit	◑	◕	KF
2.2	Aktionsplan Internationale Standards	◕	◑	MF
3.1	Pilotprogramm Risikoforschung	◕	◑	KF
3.2	EU-Beihilferichtlinien Risikoforschung	◕	◑	MF
4.1	Einfuhr- und Marktzugangsbeschränkungen	◑	●	MF
4.2	Informationsreihen und -kampagnen IPR	◑	◕	KF
5.1	Konkurrenzsituationen Wirtschaft/Forschung	◕	◑	MF
5.2	Ausgründungen (Spin-offs)	◕	◕	MF
5.3	Gründernetzwerk „IT-Sicherheit“	◑	◕	KF
5.4	Gründerstipendium „IT-Sicherheit“	◕	◕	KF
5.5	KfW-Gründerprogramm „IT-Sicherheit“	◕	◕	MF
5.6	Gründerpatenschaften „IT-Sicherheit“	◕	◑	MF
5.7	Förderwettbewerb „Kooperation IT-Sicherheit“	◑	◑	KF
6.1	Leuchtturmprojekte IT-Sicherheit	◕	◑	LF
7.1	Anreize für Einsatz „sicherer“ IT	◕	◔	MF
7.2	Elektronischer Geschäftsverkehr	◕	◑	MF
8.1	Ziele für Exportunterstützung	◕	◔	MF
8.2	Exportkontrollprozess	◕	◔	MF
8.3	Neuausrichtung ITSMIG	●	◑	MF
8.4	Delegationsreisen	◑	◕	MF
8.5	Zentrale Kontaktstelle bei der GTAI	◑	◕	KF
9.1	„Branchenforum IT-Sicherheit“	●	◕	KF
9.2	Messestandort Deutschland zur IT-Sicherheit	◕	◑	MF
9.3	Aktionsplan „Auslandsmessen IT-Sicherheit“	◕	◕	KF
9.4	Positionierung des Themas IT-Sicherheit	◑	◕	KF
10.1	Evaluierung Aufklärungs- und Informationskampagnen	◑	◕	KF
10.2	Hochrangige Medienkampagne zur IT-Sicherheit	◕	◕	KF
11.1	Finanzierungsmöglichkeiten der Bundesregierung	◑	◕	KF
11.2	Steuerrechtliche Behandlung von Risikokapital	◕	◑	MF
11.3	Stiftung/Risiko-Investmentfonds „IT-Sicherheit“	●	◑	MF

● Sehr hoch ◕ Hoch ◑ Mittel ◔ Niedrig ○ Kein

LF - Langfristig (>1 Jahr) MF - Mittelfristig (6 Monate - 1 Jahr) KF - Kurzfristig (0 - 6 Monate)

[164] Booz & Company-Analyse

Basierend auf dieser Bewertung wurden die 36 Einzelmaßnahmen in die folgende Matrix eingeordnet. Bei dieser Einordnung haben sich vier Gruppen (Cluster) herausgebildet, die bei der späteren Umsetzung weitergeführt werden. Die Einordnung der Maßnahmen in die Matrix lässt zudem eine einfache Priorisierung der Maßnahmen bzw. der Gruppen erkennen. (Die in der folgenden Matrix enthaltenen Nummerierungen der Einzelmaßnahmen entsprechen der Nummerierung aus der Tabelle 17)

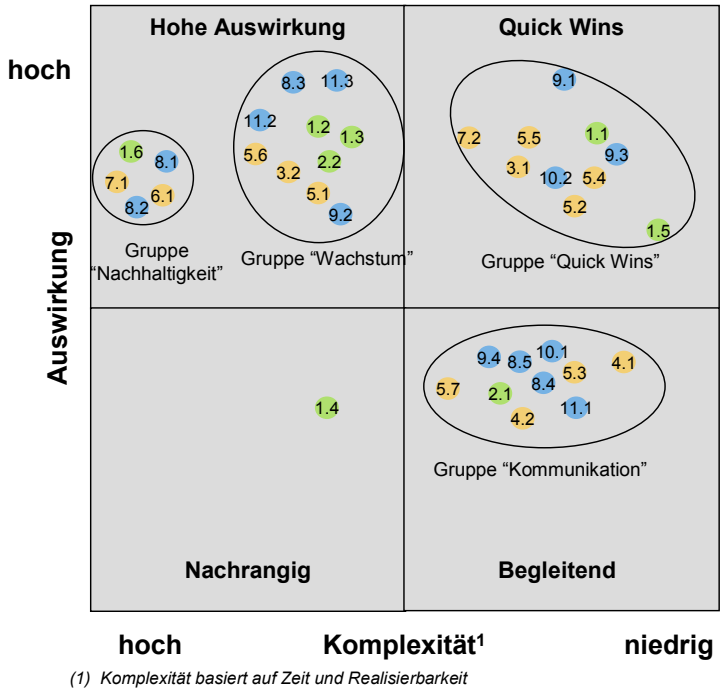


Abbildung 46: Matrixdarstellung der Bewertungen der 36 Einzelmaßnahmen[165]

7.7.2 Bewertung

Die Einzelmaßnahmen bilden im Wesentlichen vier Gruppen (Cluster), die die Umsetzung der Maßnahmen vereinfachen werden. An vorderster Stelle steht dabei die Gruppe „Quick Wins", die Maßnahmen enthält, die mit vergleichsweise geringem Aufwand innerhalb kurzer Zeit eine hohe Wirkung entfalten können. Darauf folgt die Gruppe „Wachstum" mit den Maßnahmen, die eine ebenso hohe Wirkung wie die „Quick Wins" versprechen, für die Umsetzung aber einen längeren Zeitraum beanspruchen. An dritter Stelle folgt die Gruppe „Kommunikation" mit den Maßnahmen, die eine geringere

[165] Booz & Company-Analyse

Wirkung entfalten, aber im gleichen Zeitraum wie die Gruppe „Wachstum“ verwirklicht werden können. Daran anschließend folgt die Gruppe „Nachhaltigkeit“ mit Maßnahmen, für die eine hohe und nachhaltige Auswirkung festgestellt wurde, die aber einen bedeutend höheren zeitlichen, finanziellen und organisatorischen Aufwand erfordern. Das Schlusslicht bildet die Einzelmaßnahme 1.4 („Experten-Austauschprogramm IT-Sicherheit“), die in keine Gruppe eingeordnet werden konnte. Auch diese Maßnahme lohnt eine Umsetzung, jedoch sollte diese aufgrund ihrer geringeren Auswirkung und ihres höheren Aufwands nur nachrangig erfolgen.

Im Folgenden werden die einzelnen Gruppen näher betrachtet und eine Bewertung vorgenommen, wie sich die Umsetzung der Maßnahmen in dieser Gruppe auf die übergeordneten Handlungsziele „Sicherung“, „Innovation“ und „Wachstum“ auswirken wird. Sollte sich dabei herausstellen, dass die aufgeführten Maßnahmen nicht ausreichen, die Ziele zu erreichen, müsste entweder über eine Erhöhung der finanziellen Ausstattung der Maßnahmen oder über weitere Maßnahmen nachgedacht werden.

Gruppe „Quick Wins“

Die Maßnahmen in dieser Gruppe, die sogenannten „Quick Wins”, sind von besonderer Bedeutung, da sie rasche Anfangserfolge ermöglichen und dadurch die Motivation der Akteure steigern, die nächste Gruppe von Maßnahmen anzugehen. Das vorrangige Ziel dieser Maßnahmengruppe ist es, günstige Voraussetzungen für eine bessere Kommunikation und Kooperation unter den Akteuren der deutschen IT-Sicherheit zu schaffen. Als wesentliche Stütze zur Erreichung dieses Ziels wird die Einrichtung des „Branchenforums IT-Sicherheit“ dienen. Dieses Forum soll sich der Kommunikation der deutschen IT-Sicherheitsanbieter untereinander sowie mit der Bundesregierung (hier vertreten durch das BMWi) widmen. Neben den Maßnahmen zur Förderung von Ausgründungen aus dem Forschungsbereich bzw. von Existenzgründungen im Bereich der IT-Sicherheit werden der Aktionsplan Auslandsmessen, der Deutsche IT-Sicherheitspreis sowie das Pilotprogramm Risikoforschung wichtige Impulse setzen, die Kooperation unter den Unternehmen zu fördern. Die hochrangige Medienkampagne IT-Sicherheit wird zudem dafür sorgen, dass der Staat seiner Vorbildfunktion nachkommt und dass diese in geeigneter Weise in der Öffentlichkeit dargestellt wird.

Tabelle 18: Übersicht der Gruppe „Quick Wins"

Gruppe	Maßnahme #	Bezeichnung der Maßnahmen	Auswir-kungen	Realisier-barkeit	Zeit-rahmen
"Quick Wins"	9.1	„Branchenforum IT-Sicherheit"	●	◕	KF
	9.3	Aktionsplan „Auslandsmessen IT-Sicherheit"	◕	◕	KF
	10.2	Hochrangige Medienkampagne zur IT-Sicherheit	◕	◕	KF
	1.1	Branchenregister IT-Sicherheit	◕	◕	KF
	1.5	Deutscher IT-Sicherheitspreis	◑	●	KF
	5.4	Gründerstipendium „IT-Sicherheit"	◕	◕	KF
	3.1	Pilotprogramm Risikoforschung	◕	◑	KF
	5.2	Ausgründungen (Spin-offs)	◕	◕	MF
	5.5	KfW-Gründerprogramm „IT-Sicherheit"	◕	◕	MF
	7.2	Elektronischer Geschäftsverkehr	◕	◑	MF

● Sehr hoch ◕ Hoch ◑ Mittel ◔ Niedrig ○ Kein

LF - Langfristig (>1 Jahr) MF - Mittelfristig (6 Monate - 1 Jahr) KF - Kurzfristig (0 - 6 Monate)

Gruppe „Wachstum"

In dieser Gruppe sind insgesamt zehn Einzelmaßnahmen zusammengefasst, die ihren Schwerpunkt in der Förderung von Wachstum haben. Den Kern dieser Maßnahmengruppen bilden die Maßnahmen zur Verbesserung der Risikokapitalausstattung für die IT-Sicherheitsbranche. Mit der Gründung einer Stiftung oder eines Risiko-Investmentfonds „IT-Sicherheit" wird die Bundesregierung in Zusammenarbeit mit der Finanzwirtschaft einen wichtigen Impuls setzen, die Wachstumspläne dieser Branche nachhaltig zu unterstützen. Die Neuausrichtung der ITSMIG e.V. wird die Maßnahmen zu einer verbesserten und auf Wachstum ausgerichteten Kommunikations- und Kooperationskultur in der deutschen IT-Sicherheitslandschaft fortführen. Die erweiterten Aufgaben der ITSMIG e.V. und die stärkere Einbindung der Regierung werden die Exportchancen in wichtigen Zielmärkten verbessern. An einer vermehrten Zahl von erfolgreichen Geschäftsabschlüssen im Ausland wird man den Erfolg dieser Maßnahmen messen können.

Tabelle 19: Übersicht der Einzelmaßnahmen der Gruppe „Wachstum"

Gruppe	Maßnahme #	Bezeichnung der Maßnahmen	Auswir-kungen	Realisier-barkeit	Zeit-rahmen
"Wachstum"	8.3	Neuausrichtung ITSMIG	●	◑	MF
	9.2	Messestandort Deutschland zur IT-Sicherheit	◕	◑	MF
	11.2	Steuerrechtliche Behandlung von Risikokapital	◕	◑	MF
	11.3	Stiftung/Risiko-Investmentfonds „IT-Sicherheit"	●	◑	MF
	5.6	Gründerpatenschaften „IT-Sicherheit"	◕	◑	MF
	5.1	Konkurrenzsituationen Wirtschaft/Forschung	◕	◑	MF
	3.2	EU-Beihilferichtlinien Risikoforschung	◕	◑	MF
	1.3	Aus- und Weiterbildungsangebot	◕	◑	MF
	2.2	Aktionsplan Internationale Standards	◕	◑	MF
	1.2	Anwendungspraxis AWG	◕	◑	MF

● Sehr hoch ◕ Hoch ◑ Mittel ◔ Niedrig ○ Kein

LF - Langfristig (>1 Jahr) MF - Mittelfristig (6 Monate - 1 Jahr) KF - Kurzfristig (0 - 6 Monate)

Gruppe „Kommunikation“

Die Einzelmaßnahmen in dieser Gruppe können nach erfolgter Umsetzung der „Quick Wins“ sowie wichtiger Maßnahmen der Gruppe „Wachstum“ weitere kurzfristige Impulse setzen und die in den ersten beiden Umsetzungswellen erzielten Erfolge weiter verstetigen. So bietet der Förderwettbewerb „Kooperation in der IT-Sicherheit“ die Möglichkeit, die mit der Gründung des Branchenforums angestoßene Verbesserung der Kommunikation und Kooperation durch konkrete Bewerbungen bei diesem Wettbewerb zu demonstrieren. Das Gründernetzwerk „IT-Sicherheit“ wird den Ergebnissen der Maßnahmen aus den Gruppen „Quick Wins“ und „Wachstum“ zur Förderung von Existenzgründungen eine eigene Kommunikationsplattform bieten. Die zentrale Kontaktstelle bei der GTAI wird das Informationsangebot über ausländische Märkte und Geschäftsgelegenheiten für die IT-Sicherheitsbranche zusammen mit der neu ausgerichteten ITSMIG e.V. weiter verbessern und damit die Exportchancen weiter ausbauen.

Tabelle 20: Übersicht der Einzelmaßnahmen der Gruppe „Kommunikation“

Gruppe	Maßnahme #	Bezeichnung der Maßnahmen	Auswirkungen	Realisierbarkeit	Zeitrahmen
“Kommunikation”	2.1	DIN-Arbeit IT-Sicherheit	◑	◕	KF
	4.2	Informationsreihen und -kampagnen IPR	◑	◕	KF
	5.3	Gründernetzwerk „IT-Sicherheit“	◑	◕	KF
	4.1	Einfuhr- und Marktzugangsbeschränkungen	◑	●	MF
	5.7	Förderwettbewerb „Kooperation IT-Sicherheit“	◑	◑	KF
	8.4	Delegationsreisen	◑	◕	MF
	9.4	Positionierung des Themas IT-Sicherheit	◑	◕	KF
	10.1	Evaluierung Aufklärungs- und Informationskampagnen	◑	◕	KF
	11.1	Finanzierungsmöglichkeiten der Bundesregierung	◑	◕	KF
	8.5	Zentrale Kontaktstelle bei der GTAI	◑	◕	KF

● Sehr hoch ◕ Hoch ◑ Mittel ◔ Niedrig ○ Kein

LF - Langfristig (>1 Jahr) MF - Mittelfristig (6 Monate - 1 Jahr) KF - Kurzfristig (0 - 6 Monate)

Gruppe „Nachhaltigkeit“

Die Maßnahmen, die in der Gruppe „Nachhaltigkeit“ zusammengefasst sind, haben alle eine hohe und nachhaltige Auswirkung auf die Handlungsziele. Jedoch ist deren Umsetzung mit höherem Aufwand verbunden, u. a. weil sie eine Abstimmung mehrerer Ressorts der Bundesregierung untereinander erfordert. Ein wichtiger Meilenstein wird ein optimierter Exportkontrollprozess sein, der der IT-Sicherheitsbranche Planungssicherheit gibt, indem er eine Bearbeitungsfrist für Anträge auf Ausfuhrgenehmigung festlegt. Weitere wich-

tige Ziele dieser Maßnahmengruppe werden sein, ein neues Leuchtturmprojekt für die IT-Sicherheit ins Leben zu rufen sowie erste Fortschritte bei der Vervollständigung der Wertschöpfungskette im IKT-Bereich im Sinne einer „vertrauensvollen Werkbank“ in Deutschland zu erzielen.

Tabelle 21: Übersicht der Einzelmaßnahmen der Gruppe „Nachhaltigkeit“

Gruppe	Maßnahme #	Bezeichnung der Maßnahmen	Auswirkungen	Realisierbarkeit	Zeitrahmen
“Nachhaltigkeit”	8.1	Ziele für Exportunterstützung	◕	◔	MF
	8.2	Exportkontrollprozess	◕	◔	MF
	1.6	Wertschöpfungskette	◕	◔	MF
	6.1	Leuchtturmprojekte IT-Sicherheit	◕	◑	LF
	7.1	Anreize für Einsatz „sicherer“ IT	◕	◔	MF

● Sehr hoch ◕ Hoch ◑ Mittel ◔ Niedrig ○ Kein

LF - Langfristig (>1 Jahr) MF - Mittelfristig (6 Monate - 1 Jahr) KF - Kurzfristig (0 - 6 Monate)

Die Maßnahme 1.4 „Experten-Austauschprogramm“ ist als einzige Maßnahme keiner Gruppe zugeordnet, da sowohl die Auswirkungen als auch die Realisierbarkeit im Vergleich zu den anderen Maßnahmen als weniger hoch eingestuft wurden. Gleichwohl sollte diese Maßnahme umgesetzt werden, da sie einen wertvollen Beitrag zur Sicherung kritischer Kompetenzen leisten wird. Insbesondere der Erfahrungssaustausch mit anderen internationalen Experten sowie die Möglichkeit zum Vergleich mit den Zertifizierungsverfahren ausländischer Stellen schaffen eine wichtige Voraussetzung für eine ständige Verbesserung der eigenen Praxis.

Tabelle 22: Einzelmaßnahme 1.4 mit Bewertung

Gruppe	Maßnahme #	Bezeichnung der Maßnahmen	Auswirkungen	Realisierbarkeit	Zeitrahmen
Keine	1.4	Experten-Austauschprogramm IT-Sicherheit	◑	◑	MF

7.7.3 Zeitlicher Rahmen

Wie bereits in Abschnitt 7.7.1 ausgeführt, sollte die Umsetzung der Maßnahmen insgesamt einen Zeitrahmen von 36 Monate nach Verabschiedung der Studie nicht überschreiten, d. h. innerhalb der laufenden 17. Legislaturperiode abgeschlossen sein. Vorrangige Priorität hat die Umsetzung der Gruppe „Quick Wins“, die unmittelbar nach der Verabschiedung der Studie durch das BMWi starten und innerhalb der ersten sechs Monate wichtige Ergebnisse liefern sollte, z. B. erste Sitzung(en) des Branchenforums IT-Sicherheit und eine erste Verleihung des Deutschen IT-Sicherheitspreises. Daran schließt sich die Umsetzung der Gruppe „Wachstum“ an, für die ein Zeitrahmen von

zwölf Monaten vorgesehen ist. Etwa sechs Monate nach Beginn der Umsetzung der Gruppe „Wachstum“ sollte mit den Gruppen „Kommunikation“ und „Nachhaltigkeit“ begonnen werden, um sicherzustellen, dass die Umsetzung aller Maßnahmen nach 36 Monaten abgeschlossen ist. Die folgende Abbildung gibt einen Überblick über den zeitlichen Rahmen sowie einer Auswahl wichtiger Meilensteine.

VORSCHLAG

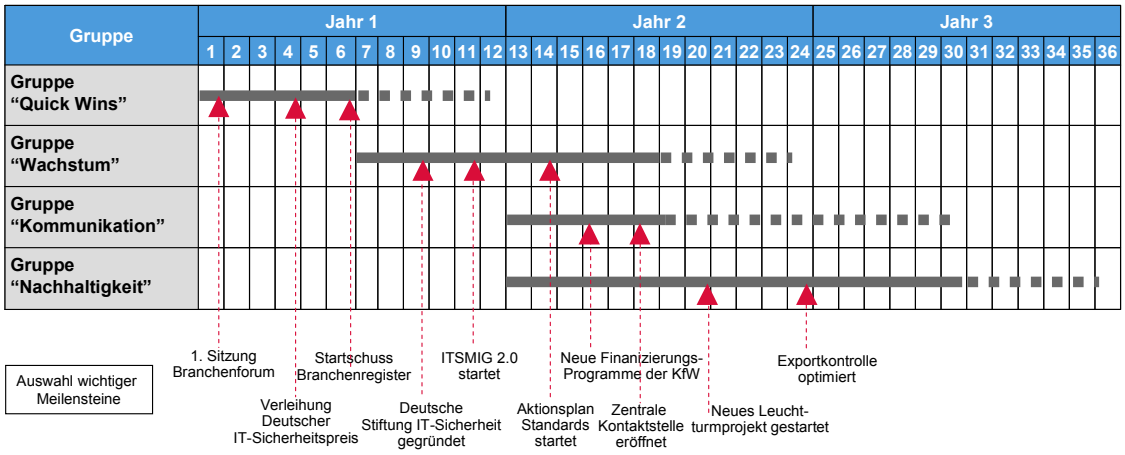


Abbildung 47: Übersicht über den Zeitrahmen mit einer Auswahl wichtiger Meilensteine[166]

Eine wichtige Voraussetzung für den Erfolg der Maßnahmen wird sein, dass die Umsetzung der Maßnahmen im Sinne eines Programmbüros zentral koordiniert und nachverfolgt wird.

[166] Booz & Company-Analyse

7.8 Zusammenfassende Bewertung

Die Bundesregierung hat die Möglichkeit, mit der konsequenten Umsetzung der Maßnahmen in den Gruppen „Quick Wins", „Wachstum", „Kommunikation" und „Nachhaltigkeit" innerhalb der kommenden 36 Monate, wichtige Wachstumsimpulse für die IT-Sicherheitsbranche zu setzen. Ziel sollte es dabei sein, das Wachstum der IT-Sicherheitsbranche in Deutschland wenigstens auf das Niveau des weltweiten Wachstums von ca. 14% in dieser Branche zu heben.

Die Schaffung einer nachhaltigen Kommunikations- und Kooperationskultur unter starker Beteiligung des Staates wird einen erheblichen Beitrag zur Erreichung dieses Wachstumsziels leisten. Ein starkes und wirtschaftsförderndes Engagement des Staates steht dabei nicht im Widerspruch zur Freiheit des Unternehmertums, sondern drückt das Selbstverständnis des Staates aus, sich selbst als „erster Unternehmer" des Staates zu sehen, die Wirtschaft im In- und Ausland tatkräftig zu unterstützen und stets für Rahmenbedingungen zu sorgen, die die Wettbewerbsfähigkeit der heimischen Unternehmen stärken. Zu diesen Rahmenbedingungen zählen neben einer effizienten Exportkontrolle vor allem Erleichterungen für die Kapitalbeschaffung.

Allerdings reichen staatliche Maßnahmen allein nicht aus. Auch die Unternehmen sind bei der Verbesserung der Kommunikation und Kooperation in der Pflicht und sollten die in diesen Maßnahmen enthaltenen Angebote konstruktiv annehmen und aktiv mit ausgestalten. Dazu zählt auch die Bereitschaft, beim Vergleich mit dem Ausland nicht stets über die besseren staatlichen Rahmenbedingungen dort Klage zu führen, sondern sich auch an der Risikobereitschaft und dem Kooperationsgeist ausländischer Konkurrenten ein Beispiel zu nehmen.

Schließlich hat die Bundesregierung auch unmittelbaren Einfluss auf die Nachfrage am Markt. Die in diesem Abschnitt nicht näher betrachteten Möglichkeiten, den Einsatz von IT-Sicherheit in der öffentlichen Verwaltung zu steigern, haben ein für die IT-Sicherheitsbranche in Deutschland nicht unerhebliches Potenzial. Der Staat sollte mit gutem Beispiel vorangehen und eine Steigerung der regulären Ausgaben für IT-Sicherheit im kommenden Jahr von 20% und in den Folgejahren von jährlich 5% anstreben, ggf. durch Ausgabenverlagerung.

8 Experten-Workshop zur Vorstellung vorläufiger Studienergebnisse

Zur Vorstellung und Diskussion der vorläufigen Ergebnisse der Studie wurden Vertreter und Experten der deutschen IT-Sicherheitsanbieter, Forschungseinrichtungen, Verbände und öffentlichen Stellen zu einem Experten-Workshop am 1. Dezember 2009 nach Bonn ins Bundesministerium für Wirtschaft und Technologie eingeladen.

Vorgestellt wurden die Zielsetzung, der Aufbau, der Betrachtungsumfang und zentrale Ergebnisse der einzelnen Kapitel der Studie. Der Schwerpunkt lag auf der Diskussion der aus der Stärken- und Schwächen-Analyse gewonnenen Erkenntnisse zu ordnungspolitischen Handlungsempfehlungen. Dies gab den Branchenvertretern, nach den bereits mit ihnen geführten Interviews zu dieser Studie, eine weitere Gelegenheit, vor der Fertigstellung des Berichts, ihre Vorstellungen und Erwartungen zur Entwicklung der IT-Sicherheitsbranche in Deutschland in die Diskussion mit dem BMWi einzubringen und die vorgeschlagenen ordnungspolitischen Handlungsoptionen zu kommentieren.

Die Diskussion zum **IT-Sicherheitsmarkt in Deutschland** ergab, dass eine Abgrenzung des Marktes für IT-Sicherheit generell schwierig, aber für die Bestimmung der deutschen Marktgröße sowie der Wachstumsbereiche notwendig ist. Die von der Studie vorgenommene Abgrenzung der betrachteten Marktsegmente entlang des Leitgedankens „Schutz von IT durch IT“ wird grundsätzlich mitgetragen, sollte aber hinsichtlich der „nicht eindeutig abgrenzbaren Bereiche“ präzisiert werden. Entsprechend ist auf die Marktdefinition in Kapitel 3 der vorliegenden Langfassung des Berichts zu verweisen:

Aus der Quantifizierung des Marktes ausgenommen wurden mittels dieser Abgrenzung Produkte und Dienstleistungen, die aus einem anderweitigen sektoralen Zuschnitt nicht herauslösbar sind. Insbesondere die Marktsegmente, in denen IT-Sicherheit ein nicht abgrenzbarer Teil einer integrierten Lösung ist, z.B. als „embedded system“, sind in der Bestimmung des Marktes im Rahmen dieser Studie nicht erfasst, da sie die statistische Beleuchtung der IT-Sicherheitsbranche als eigenen Wirtschaftszweig unmöglich gemacht hätten. Allerdings wurde im Hinblick auf die fehlende Weltmarktdominanz der deutschen IT-Sicherheitsbranche insgesamt darauf hingewiesen, dass gerade die Verzahnung mit der starken deutschen Gesamtwirtschaft eine Stärke nati-

onaler Anbieter, insbesondere der KMU sei bzw. sein könnte. Zumal derart eingebundene integrierte Lösungen unabhängig von der Weltmarktstärke der Anbieter den Dynamiken des entsprechenden Sektors, etwa der Automobilindustrie folgen und sich dabei beide Seiten gegenseitig stärken können. Bei der Marktabgrenzung würde eine Verschiebung der Definitionsweite das Marktvolumen signifikant vergrößern zu Lasten der Trennschärfe und der Eigendynamik des (in diesem Bericht beleuchteten) Kernbereichs der IT-Sicherheit. Gleichwohl muss betont werden, dass es sich in diesem Bereich um einen bedeutenden Zukunftsmarkt handelt, der für die deutschen IT-Sicherheitsanbieter, auch aufgrund der Größe und der Bedeutung einiger Sektoren – wie etwa der deutschen Automobilindustrie – in Zukunft eine zunehmend wichtige Rolle spielen dürfte. Dies könne auch im Rahmen einer Anwenderbefragung beleuchtet werden.

Die Teilnehmer stimmten mit der Analyse überein, dass die **deutschen IT-Sicherheitsanbieter** durch den hohen Anteil kleiner und mittlerer Unternehmen sehr heterogen aufgestellt sind und keine nach Umsatz- und Mitarbeiterzahlen signifikante Größe im weltweiten Vergleich besitzen. Den daraus resultierenden Größennachteilen bei Vermarktung und Marktpräsenz stehen allerdings eine wettbewerbsbedingt höhere Flexibilität und Innovationskraft der KMU gegenüber. So haben die deutschen Anbieter insbesondere in den Marktsegmenten Identitäts- und Zugriffsverwaltung, Kryptographie, Firewall, Antivirus und Intrusion Detection große technologische Kompetenzen vorzuweisen, die in die Neuentwicklung von innovativen High-End-Produkten fließen.

Die 18 in der Studie näher untersuchten Unternehmen repräsentieren einen IT-Sicherheits-Umsatz in Deuschland von ca. 500 Mio. Euro. Eine Aussage inwieweit damit der Gesamtmarkt von 2,5 Mrd. Euro repräsentativ abgedeckt ist, kann allerdings nicht ohne weiteres getroffen werden, da Umsätze deutscher Firmen im Ausland und Umsätze in anderen Geschäftsbereichen teilweise nicht eindeutig abgrenzbar sind. Zum Teil wurden Angaben zum Umsatz von den Unternehmen nicht herausgegeben.

Hinsichtlich der dargestellten Bedrohungslage betonten die Unternehmen, dass die steigende Relevanz der Branche nicht vorrangig durch neue Bedrohungen getrieben sei, sondern durch die steigende Bedeutung von IT für die gesamtwirtschaftlichen Prozesse, die damit zunehmend den Bedrohungen ausgesetzt sind und eine Potenzierung des Bedrohungspotentials bewirken.

Zu den vorgestellten 11 Handlungsoptionen mit 36 Einzelmaßnahmen aus den drei Zielbereichen „Sicherung kritischer Kompetenzen", „Innovation" und „Wachstum" wurde einleitend von den Teilnehmern angemerkt, dass eine genaue Definition und Festlegung der kritischen Kompetenzen wünschenswert wäre. Dies bedürfte einer nicht zuletzt technologisch orientierten Bestimmung der relevanten Felder für „kritische Kompetenzen". Nur aufbauend auf solch einer detaillierteren Bestimmung, so der Workshop-Teilnehmerkreis, sei es möglich, die einzelnen Handlungsempfehlungen zu kritischen Kompetenzen weiter zu spezifizieren.

Hinsichtlich des **Handlungsziels „Sicherung kritischer Kompetenzen"** wurde die vorgeschlagene Maßnahme zur Stärkung der deutschen Beteiligung in den internationalen Standardsetzungsgremien besonders hervorgehoben. Die Teilnehmer sprachen sich mehrheitlich dafür aus, dieses Thema verstärkt voranzutreiben, da die Standardsetzung einen bedeutenden Einfluss auf die Absatzchancen in internationalen Märkten hat. Der Vorschlag zur wirtschaftspolitischen Begleitung bei der Schließung bestehender Lücken in der Wertschöpfungskette für eine „vertrauensvolle Werkbank" wurde diskutiert und angesichts des fortgeschrittenen Verlusts von Teilbereichen als wenig aussichtsreich eingestuft – hier müsste insbesondere im Hinblick auf den international als Einheit wahrgenommenen europäischen Wirtschaftsraum eine europäische Vervollständigung im internationalen Wettbewerb verfolgt werden.

Mit Blick auf das **Handlungsziel „Innovation"** hoben die Teilnehmer insbesondere die Vorbild- und Vorreiterrolle des Staates hervor, den Einsatz innovativer IT-Sicherheitsprodukte auf seinen eigenen IT-Systemen zu verstärken. Kritisch beurteilt wurden dabei Tendenzen zum „Insourcing durch Behörden". Als Beispiel wurde hierbei die „Rück-Verstaatlichung" der Bundesdruckerei angeführt, die dem Markt Wachstumsimpulse im Rahmen öffentlicher Auftragsvergabe entzieht.

Mit Bezug auf die Einfuhr- und Marktzugangsbeschränkungen wurde von den Teilnehmern auf die uneinheitliche Anwendungspraxis innerhalb der EU bei Zertifizierungen hingewiesen. Die Unternehmen beklagten, dass eine Zertifizierung durch das BSI einen ungleich höheren zeitlichen und finanziellen Aufwand erfordere und schlugen ergänzend Sicherheitspreise bzw. eine bessere Vermarktung der Sicherheitsvorteile deutscher Produkte vor. Die Teilnehmer wünschten sich von der Bundesregierung Verbesserungen insbeondere bei der Verfahrensdauer und den Zertifizierungsanforderungen , um ü-

ber eine BSI Zertifizierung die Vorteile der gegenseitigen Anerkennung der Zertifizierungen in ausländischen Märkten, vor allem innerhalb der EU, besser nutzen zu können. Gleichzeitig wurde aber vor voreiligen Maßnahmen gewarnt, um den Effekt der Zertifizierung als Mittel zur Abwehr von Billiganbietern in Deutschland nicht leichtfertig aufzugeben.

Der Vorschlag der Studie zu einer Gründer-Initiative mit Aufbau von Gründernetzwerken und staatlicher Förderung von Ausgründungen wurde von einigen Teilnehmern kritisch beurteilt. Die Gründerinitiative fördere zwar Innovationen, zugleich würde sie die in der Studie festgestellte Zersplitterung der KMU-Landschaft in der deutschen IT-Sicherheitsbranche weiter verstärken. Von Seiten des BMWi wurde dem entgegnet, dass mehr Wettbewerb die deutsche IT-Sicherheitsbranche im Ganzen stärken würde. Eine politische Initiative zur Schaffung eines nationalen Champions findet nicht die Zustimmung der Bundesregierung, jedoch wurde vom BMWi eine bessere Förderung von Innovationsclustern, zum Beispiel durch einen Wettbewerb für Modell-Regionen, für denkbar erachtet.

Insgesamt wurde eine Schwerpunktsetzung auf das **Handlungsziel „Wachstum“** sowie die Betonung auf die Stärkung der Kommunikations- und Kooperationsbereitschaft mit und innerhalb der deutschen IT-Sicherheitswirtschaft eingefordert.

Insbesondere die Maßnahmen zur Verbesserung der Exportunterstützung, zum Beispiel durch Optimierung und Beschleunigung des Exportkontrollverfahrens, sowie einer Neuausrichtung der ITSMIG-Initiative wurden begrüßt und deren kurzfristige Umsetzung erbeten.

Die Teilnehmer beklagten zudem, dass die Förderung von Geschäftstätigkeiten im Ausland durch die deutschen Botschaften nur dann gut funktioniere, wenn es nur einen einzigen deutschen Bewerber gäbe. Wichtig wäre jedoch, dass diese Unterstützung auch dann erfolge, wenn mehr als ein Unternehmen sich um einen Auftrag im Ausland bemühe, und zwar für alle beteiligten Unternehmen.

Das vorgeschlagene Branchenforum zur Förderung der Kommunikations- und Kooperationsbereitschaft wurde von den Teilnehmern als hilfreiche Maßnahme gesehen und könnte mit dem Vorschlag eines Innovations-Kongresses verbunden werden.

Das Thema Kooperationsbereitschaft der Unternehmen wurde ebenfalls intensiv erörtert und von einigen Teilnehmern die Notwendigkeit hervorgehoben, die erkannte Schwäche der deutschen Anbieter auf diesem Gebiet nicht durch rein deutsche Maßnahmen zu beheben, sondern sich Kooperationspartner auf europäischer Ebene zu suchen, um im internationalen Wettbewerb die erforderlichen Skaleneffekte erzielen zu können.

Von Seiten der Teilnehmer wurde angeregt, neben der FuE-Förderung ein Förderprogramm zur Verbesserung der Marketing- und Vertriebs-Kompetenzen in der deutschen IT-Sicherheitsbranche zu schaffen. Ziel wäre, bekannte Schwächen in diesem Bereich abzubauen und die Firmen zu befähigen, mit wettbewerbsfähigen Produkten frühzeitiger und aggressiver in den Vertriebszyklus einzusteigen.

Insgesamt wünschten sich die Teilnehmer ein insgesamt stärkeres Engagement des Staates bei der Exportförderung und die prioritäre Umsetzung der Maßnahmen, die sich auf das Wachstum auswirken und kurzfristig realisiert werden können.

9 Anhang: Detaillierte Analyse der Bedrohungslage

9.1 Aktuelle Schwachstellen und Bedrohungen von IT-Systemen

9.1.1 Sicherheitslücken

Sicherheitslücken in komplexen Produkten wie Software können von Angreifern mit so genannten Exploits ausgenutzt werden, um Benutzer- oder sogar Administratorrechte zu erlangen.[167] Schad- und Malware-Programme können nur Schaden anrichten, wenn sie tatsächlich eine Sicherheitslücke ausnutzen.

Für rund die Hälfte der neu gemeldeten Schwachstellen wurde von den Herstellern der Produkte kein Update zur Behebung des Sicherheitsproblems bereitgestellt. Der Zeitraum zwischen dem Bekanntwerden einer neuen Sicherheitslücke und der Veröffentlichung eines Exploits wird zunehmend kürzer so, dass notwendige Programmupdates nicht schnell genug zur Verfügung gestellt oder andere Schutzmaßnahmen entwickelt werden können. So kam es 2008 zu einem deutlichen Anstieg so genannter **Zero-Day-Angriffe,** d.h. von Angriffen, bei denen eine Sicherheitslücke noch vor oder am gleichen Tag der öffentlichen Bekanntmachung ausgenutzt wird[168]. Der raschen Veröffentlichung von Schwachstellen bzw. Sicherheitslücken z.B. durch das BSIaber auch durch die Industrie und staatliche Aufsichtbehörden kommt daher eine besondere Bedeutung zu.

Tabelle 23: Einschätzung Gefährdungsentwicklung für Sicherheitslücken

	2007	2009	Prognose
Gefährdungsentwicklung	↑	↑	→

Zunehmende Gefahr geht von den so genannten **Drive-by-Downloads** aus. Angreifer manipulieren dabei vermehrt auch seriöse Webseiten, um vom Nutzer unbemerkt einen Schadcode auf den PC zu schleusen. Ausgenutzt werden hierzu Sicherheitslücken im Webbrowser oder in installierten Zusatzkomponenten (Plug-Ins). Nach Erkenntnissen des BSI existieren die meisten

[167] Secunia Monthly Report, 2008
[168] BSI, Die Lage der IT Sicherheit in Deutschland, 2009

Schwachstellen im Zusammenhang mit Webbrowsern in ActiveX-Steuerelementen (zum Beispiel Java Applets oder Flash-Filme), die zur Darstellung von aktiven und multimedialen Inhalten verwendet werden..

Tabelle 24: Einschätzung Gefährdungsentwicklung für Drive-by-Downloads

	2007	2009	Prognose
Gefährdungsentwicklung	-	↑	↑

9.1.2 Schadprogramme

Mit „Schadprogramm“ (Malware) wird Software bezeichnet, die sich unbemerkt in einem Computersystem installiert, um die Vertraulichkeit, Integrität und Verfügbarkeit von Nutzerdaten, Anwendungen sowie Betriebssystemen zu kompromittieren. Gängige Formen von Schadprogrammen sind **Viren, Würmer, Trojaner, Key Logger** (Aufzeichnung von Tastaturanschlägen), **Rootkits**[169] und Prozesse um Dateien zu verstecken sowie “malicious mobile code”. Viele der infizierten Computer sind über sogenannte “Botnets” miteinander verbunden. Über diese Botnets erfolgt die Verbreitung von Spam, der Zugang zu gefälschten Webseiten zur Erlangung vertraulicher Zugangsdaten, der Angriff auf Webseiten sowie sogenannter Klick-Betrug.[170]

Die Entwicklungszyklen von Schadprogrammen werden immer kürzer. Nach Angaben des amerikanischen Anbieters für IT-Sicherheitssoftware Symantec kam es bei Bedrohungen durch Schadprogramme in 2008 zu einem deutlichen Anstieg. In diesem Zeitraum gab die Firma 1.656.227 neue Signaturen[171] für bösartigen Code heraus, eine Steigerung von 265% gegenüber 2007 mit 624.267 neuen Signaturen (vgl. Abbildung 48).

[169] Software, die nach dem Einbruch in ein Softwaresystem auf dem kompromittierten System installiert wird, um zukünftige Logins des Eindringlings zu verbergen
[170] OECD, Economics of Malware, 2008
[171] werden von Antivirus-Programmen zur Identifizierung von Viren genutzt

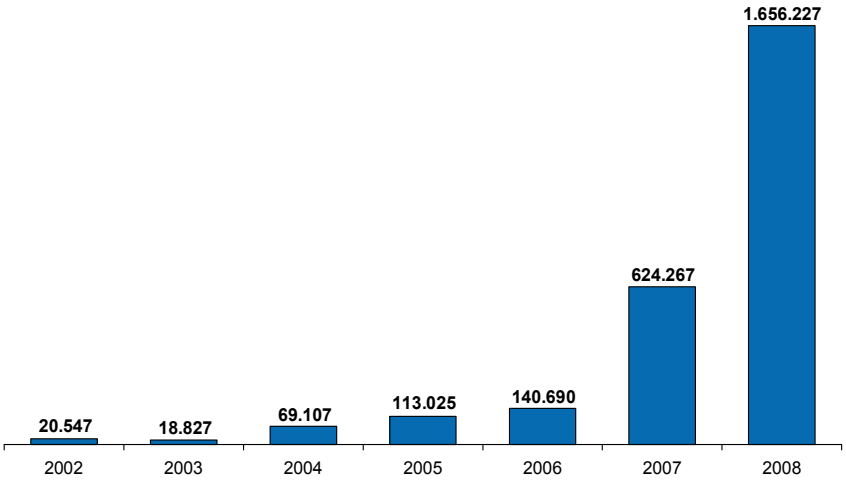


Abbildung 48: Neue Signaturen für bösartige Codes[172]

Die Einordnung von Schadprogrammen in die verschiedenen Kategorien wie Viren, Würmer, Trojanische Pferde oder Bots wird jedoch zunehmend schwierig. Die meisten Schadprogramme sind modular aufgebaut und verfügen über mehrere Schadfunktionen. So kann beispielsweise ein Trojanisches Pferd über Backdoor- und Spywarefunktionen verfügen, einen Keylogger verwenden und den befallenen Rechner zusätzlich an ein Botnet anschließen. Zudem verfügen die meisten Schadprogramme über Update-Funktionen, so dass neue Programme oder Tarnmechanismen jederzeit nachgeladen werden können. Bot-Rechner, die mehrfach am Tag mit Updates versorgt werden, sind daher Standard. Hierzu zählen auch polymorphe serverseitige Viren wie zum Beispiel der „TroGen“, ein Trojaner-Echtzeitgenerator, der jeden Namen annehmen kann und sich bei jedem Aufruf verändert.

Eine wichtige Möglichkeit diesen Echtzeitbedrohungen zu begegnen, ist die pro-aktive Erkennung von Viren ohne konkretes Signatur-Update. Solche „Frühwarnalgorithmen“ sind in der Lage, einen erheblichen Anteil der Gefahrenpotenziale in Echtzeit zu erkennen und zu eliminieren und somit das Zeitfenster für einen erfolgreichen Angriff gegen null laufen zu lassen. Damit ist es auch möglich den Aufwand für die serverseitigen Updates zu reduzieren.

Schadprogramme werden zunehmend gezielter eingesetzt als früher und nicht mehr wahllos an möglichst viele Opfer verteilt. Wurden vor zwei Jahren

[172] Symantec Corporation, 2009

die meisten Schadprogramme per E-Mail verschickt, erfolgt die Verbreitung inzwischen in großer Zahl durch unbewusstes Herunterladen beim bloßen Anschauen der von Angreifern präparierten Webseiten (Drive-by-Downloads). Untersuchungen zufolge wurden im Zeitraum von Januar bis März 2008 durchschnittlich 15.000 infizierte Webseiten pro Tag entdeckt. Davon gehörten 79% zu grundsätzlich harmlosen Internetangeboten.[173]

Trojanische Pferde installieren sich heimlich und bringen einen einzelnen Rechner unter die Kontrolle eines Angreifers. Sie sind das wichtigste Werkzeug, um Passwörter zu stehlen oder ein Opfer gezielt auszuspionieren. Wurden dabei früher hauptsächlich zentrale Server eines Unternehmens oder einer Behörde angegriffen, um das dahinter liegende Netz auszuspionieren, haben sich die gezielten Angriffe auf einzelne Arbeitsplatzrechner verlagert. Zunehmend wird hierzu „Social Engineering" angewendet, bei dem sich Angreifer durch gezielte persönliche Kontaktaufnahme (z.B. in Chatforen oder anderen sozialen Onlineplattformen) zu Mitarbeitern in deren Vertrauen einschleichen. Dies zeigt, dass die Wirtschaftskriminalität zunehmend zu nachrichtendienstlichen Methoden greift. Auf diese Weise werden Informationen ausgespäht, präparierte E-Mails ausgetauscht oder Mitarbeiter dazu gebracht eine präparierte Webseite zu öffnen bzw. einen manipulierten Datenträger (zum Beispiel USB-Stick) anzuschließen. Diese Form von Angriff wird im Verfassungsschutzbericht 2009 der Bundesregierung besonders hervorgehoben, und zwar nicht nur als Methode der Wirtschaftskriminalität, sondern auch als eine Methode der Nachrichtenbeschaffung durch die Geheimdienste fremder Regierungen, insbesondere Russland und China. Bei Angriffen über manipulierte E-Mail-Anhänge werden aufgrund der weiten Verbreitung am häufigsten Microsoft Office-Dateien (wie Word oder PowerPoint) oder PDF-Dateien missbraucht.

Tabelle 25: Einschätzung Gefährdungsentwicklung für Schadprogramme

Gefährdungsentwicklung	2007	2009	Prognose
Trojanische Pferde	↑	↑	↑
Viren Würmer	↓	↓	⇉

[173] BSI, Die Lage der IT Sicherheit in Deutschland, 2009

Spyware	↑	↑	→

9.1.3 DoS / DDoS -Angriffe

Als **Denial of Service** (DoS) wird ein Angriff auf ein IT-System bezeichnet, welcher einen oder mehrere seiner Dienste arbeitsunfähig macht, in der Regel durch Überlastung. Erfolgt der Angriff verteilt von einer größeren Anzahl von fremden Systemen aus, so spricht man von **Distributed Denial of Service** (DDoS).

In jüngster Vergangenheit haben vor allem Großschadensereignisse, wie der Estland-Vorfall 2007 sowie die Angriffe auf Georgien im Jahr 2008 in der Öffentlichkeit für Aufmerksamkeit gesorgt. Im Falle Estland wurden durch DoS Angriffe die Webseiten von Regierungsstellen, Banken, Zeitungen und anderen Unternehmen über Wochen beeinträchtigt. Im Georgien-Vorfall waren die Web 2.0 Anwendungen Twitter, Facebook und der Blogdienst Livejournal durch DDoS Angriffe auf das Profil eines georgischen Nutzers für mehrere Stunden nicht verfügbar.

DoS und DDoS Angriffe erfolgen häufig mittels Backdoor-Programmen, die sich von alleine auf anderen Rechnern im Netzwerk verbreiten und dem Angreifer durch solche Botnets weitere Wirte zum Ausführen seiner Angriffe bringen.

Insbesondere bei DoS/DDoS-Angriffen nehmen ideologisch bzw. politisch motivierte Aktionen weiter zu[174]. Grundsätzlich stellen DoS-Angriffe eine Bedrohung für alle Arten von IT-Systemen dar.

Tabelle 26: Einschätzung Gefährdungsentwicklung für DoS/DDoS-Angriffe

	2007	2009	Prognose
Gefährdungsentwicklung	→	↑	↑

9.1.4 Unerwünschte E-Mails (Spam)

Am Netzübergang der Bundesbehörden konnte festgestellt werden, dass von 100 empfangenen E-Mails im Durchschnitt gerade einmal 1,5 Mails vom Empfänger erwünscht sind.[175] Bei unzureichenden Filtermethoden kann der Erhalt von massenhaft versendeten Spam-Mails unvermittelt in einen DoS-Angriff

[174] BSI, Die Lage der IT Sicherheit in Deutschland, 2009
[175] BSI, Die Lage der IT Sicherheit in Deutschland, 2009

übergehen. Neben lästigen Spam-Mails zu Werbezwecken, gibt es zunehmend Mails, die mit betrügerischer Absicht versendet werden. Dazu gehören E-Mails, die auf Phishing-Seiten verweisen, finanzielle Lockangebote sowie Mails, die zum Spenden animieren sollen oder mit schädlichen Anhängen oder Links versehen sind.

Tabelle 27: Einschätzung Gefährdungsentwicklung für Spam

	2007	2009	Prognose
Gefährdungsentwicklung	↑	↑	↑

9.1.5 Botnets

Wie in 4.4.1.2 dargestellt, fallen Botnets unter die Kategorie der Schadprogramme. Sie stellen in vielfältiger Weise eine Bedrohung der IT-Sicherheit dar. Im April 2009 sollen fast zwei Millionen PCs von Kriminellen aus der Ukraine unter ihre Kontrolle gebracht worden sein. Mitarbeiter des Sicherheitsunternehmens Finjan hatten im Rahmen einer Studie einen Command & Control Server (C&C-Server) ausfindig gemacht, über den alle infizierten Rechner gesteuert wurden. Über 45% der infizierten Rechner wurden in US Regierungsdomains (*.gov) lokalisiert, etwa 4% in Deutschland. Mit Hilfe des entdeckten C&C-Server seien die Kriminellen in der Lage, nahezu jeden Befehl auf den infizierten PC ausführen zu lassen, insbesondere E-Mails zu lesen, Dateien zu kopieren oder Tastenanschläge aufzuzeichnen. Vor allem aber ist es ihnen möglich, die gekaperten PC zum Versenden von Spam-Mails zu verwenden.[176]

Die Infektion eines PCs mit Bots erfolgt zum Beispiel unter Ausnutzung bekannter Sicherheitslücken in Systemdiensten und Applikationen (siehe auch 4.4.1.1). Eine weitere effektive Infektionsmethode ist der Einsatz von Social Engineering, um den Anwender zu einer unbedachten Handlung, wie dem Klicken auf bösartige E-Mail-Links bzw. Instant-Messaging-Nachrichten oder der Ausführung von E-Mail-Anhängen, zu verleiten. In jüngster Zeit ist außerdem zu beobachten, dass legitime, vertraute und stark frequentierte Webseiten manipuliert werden, um sie für die Verbreitung von Schadcode zu missbrauchen.

[176] Spiegel Online, 2009

Tabelle 28: Einschätzung Gefährdungsentwicklung für Botnets

	2007	2009	Prognose
Gefährdungsentwicklung	→	↑	↑

9.1.6 Identitätsdiebstahl

Mittels Identitätsdiebstahl versuchen Kriminelle, personenbezogene Daten zu missbrauchen, um sich damit einen – meist finanziellen – Vorteil zu verschaffen. Während in den letzten Jahren vorwiegend Nutzerdaten für Online-Banking und Kreditkarten für betrügerische Finanztransaktionen missbraucht wurden, werden mittlerweile nicht mehr nur kurzfristige Zugangs- und Transaktions-Daten gesammelt. Informationen zur Identität wie etwa Geburtsdatum, Anschrift und Führerscheinnummern sind ebenfalls Ziel der Angreifer. Die Popularität von Social Networks, in denen Mitglieder freiwillig eine Vielzahl privater Daten preisgeben, vereinfacht Phishing und Datenmissbrauch erheblich.

Spyware-Programme spionieren das Surf-Verhalten einer Person im Internet aus, um Benutzerprofile zu erstellen. Diese werden dann entweder vom Spyware-Ersteller selbst genutzt oder an kommerzielle Firmen verkauft, damit diese zielgerichtet Werbeeinblendungen platzieren können. Besonders gefährlich ist es, wenn die Spyware auch Anmeldedaten wie Benutzername oder Passwort heimlich mitprotokolliert und dann überträgt. Mit diesen Daten kann ein Identitätsdiebstahl ermöglicht werden. Zur Entfernung von Spyware müssen spezielle Anti-Spyware-Programme eingesetzt werden, da nur wenige Virenschutzprogramme dies ebenfalls leisten.

Tabelle 29: Einschätzung Gefährdungsentwicklung für Identitätsdiebstahl

	2007	2009	Prognose
Gefährdungsentwicklung	↑	↑	↑

9.1.7 Betrügerische Webangebote

Bei betrügerischen „Webangeboten“ werden Internetnutzern über vermeintliche gratis Informationsangebote im Internet ohne besonderen Hinweis kostenpflichtige Dienste verkauft. Die bekanntesten Fälle sind die sogenannten **Abofallen**, bei denen seriös erscheinende Webseiten dem Nutzer im Rahmen eines vermeintlich kostenlosen Tests ein Informationsangebot zur Verfügung

gestellt wird. Häufig wird nur im Kleingedruckten erwähnt, dass der Anwender bei Inanspruchnahme des Angebots ein Abo mit längerer Laufzeit abschließt oder aber eine Nutzungsgebühr zu zahlen hat.

Dieser Bedrohung haben sich Hersteller von Anti-Onlinebetrugs-Software gewidmet (z.B. Officer Blue), die sich auf Datenbanken mit zum Teil über 1 Million Einträgen betrügerischer Webangebote in Deutschland stützen.

Tabelle 30: Einschätzung Gefährdungsentwicklung für betrügerische Webangebote

	2007	2009	Prognose
Gefährdungsentwicklung	-	↑	→

9.1.8 Materielle Sicherheit, Innentäter, Irrtum und Nachlässigkeit

Aktuelle Studien sind zu dem Ergebnis gekommen, dass die größte Gefahr für Unternehmen sowie für die öffentliche Verwaltung von den aktiven sowie ehemaligen Mitarbeitern ausgeht. Im Lagebericht 2009 des BSI werden die eigenen Mitarbeiter mit 24% als die größte Tätergruppe angegeben.[177]

Das CIO Magazine, in seiner gemeinsam mit der Unternehmensberatung PricewaterhouseCoopers (PWC) erstellten Studie, bei der 2008 weltweit über 7.000 Führungskräfte zum Thema IT-Sicherheit befragt wurden, kam zu dem Ergebnis, dass lediglich 59% der Befragten über eine IT-Sicherheitsstrategie im Unternehmen verfügen. Dabei hat die Studie ergeben, dass diejenigen, die eine IT-Sicherheitsstrategie verfolgten sowie diejenigen, die das Thema IT-Sicherheit in der Chef- bzw. Vorstandsetage etablierten, deutlich weniger Vorfälle zu verzeichnen hätten. Dies verdeutlicht den hohen Stellen wert der Awareness-Bildung.

9.1.9 Angriffe mit nachrichtendienstlichen Methoden

Nachrichtendienstliche Methoden werden nicht mehr nur im Bereich der staatlicher IT-Kriminalität angewandt, sondern auch von Firmen und kriminellen Organisationen.

Laut Verfassungsschutzbericht 2008 ist die Bundesrepublik Deutschland wegen ihrer geopolitischen Lage, ihrer wichtigen Rolle in EU und NATO sowie als Standort zahlreicher Unternehmen der Spitzentechnologie mit Weltmarktführung für fremde Nachrichtendienste (insbesondere die Russische Födera-

[177] Corporate Trust, Gefahrenbarometer 2010, 2009

tion, die Volksrepublik China sowie Länder des Nahen, Mittleren und Fernen Ostens sowie Nordafrikas) attraktiv.[178]

Klassische Schutzmaßnahmen wie Virenschutzprogramme und Firewalls sind laut BSI nicht mehr ausreichend, um einen wirksamen Schutz gegen die aggressiven Methoden der Wirtschaftsspionage zu erreichen. In diesem Zusammenhang sehen deutsche Unternehmen meist eine höhere Bedrohung für die deutschen Standorte, als bei den ausländischen Töchtern oder Niederlassungen. Sowohl für Deutschland (53,1%) als auch weltweit (37,2%) wurde die Gefahr durch Informationsabfluss oder Spionage am höchsten eingeschätzt.[179]

9.2 Neue Bedrohungsszenarien in ausgewählten Technologien

9.2.1 Voice over IP (VoIP)

Das Spektrum der Bedrohungen im Bereich VoIP reicht von **SPIT-Attacken** (Spam over Internet Telephony) über das Abhören durch unbemerktes Umleiten auf einen Fremdserver (Man in the Middle) bis hin zu Spyware, Würmern und Viren. Da sich Telefone und Computer im gleichen Netz befinden, kann jeder PC oder Laptop zum Einfallstor für Angriffe werden. Zudem kommt es immer häufiger zu „Spoofing"-Angriffen, bei denen sich Unbefugte über gefälschte IP-Adressen am VoIP-Server eines Unternehmens anmelden und auf dessen Kosten telefonieren.

Während sich diese Probleme noch durch leistungsstarke Abwehrsysteme wie Firewalls, Intrusion-Detection- und Verschlüsselungslösungen in den Griff bekommen lassen, entsteht durch die Konvergenz von Daten und Sprache auf einer gemeinsamen Infrastruktur noch eine ganz andere Bedrohung, für die es keine einfach zu handhabende Lösung gibt: Im Fall einer Netzstörung versagen E-Mail, Internet und Telefon gleichzeitig. Der Einsatz von VoIP in Unternehmen zieht daher angemessene Pläne für Disaster Recovery (Wiederherstellung des Betriebs im Notfall) und Business Continuity (ununterbrochener Geschäftsablauf) mit sich. Denn die Folgen eines Netzausfalls sind in konvergenten Architekturen weitaus dramatischer als bei separaten Netzen.[180]

---

[178] Bundesministerium des Innern, Verfassungsschutzbericht 2008 Vorabfassung, 2008
[179] Corporate Trust, Gefahrenbarometer 2010, 2009
[180] Stefan Mutschler/wg, LANLINE.de, 2008

Tabelle 31: Einschätzung Gefährdungsentwicklung für Voice over IP

	2007	2009	Prognose
Gefährdungsentwicklung	↑	→	→

9.2.2 Mobile Kommunikation

Die Verfügbarkeit mobiler breitbandiger Internetverbindungen[181] wird in den kommenden Jahren weiter steigen und mit ihr die Verbreitung von Smartphones, PDAs und Subnotebooks. Dabei werden mobile Endgeräte in ihrer Softwareausstattung immer PC-ähnlicher. Aus diesem Grund und mit zunehmender mobiler Nutzung von Internet- und Datenkommunikationsdiensten steigt auch die Gefahr von Virus-Attacken und Angriffen mit trojanischen Pferden stark an.

Des Weiteren werden in Deutschland immer noch unverschlüsselte oder schwach verschlüsselte (WEP) WLAN-Verbindungen betrieben, welche die Gefahr von „wardriving" und **Man-In-The-Middle (MITM)** Attacken erhöhen. Bei MITM-Attacken, auch Janusangriff genannt, täuscht der Angreifer dem Kommunikationspartner unbemerkt das jeweilige Gegenüber vor und kann somit die Kommunikation und den Datenverkehr ausspähen.

Die IT-Sicherheitsfirma Kaspersky hat auf der CeBit 2006 durch „wardriving" den Status der auf der Messe eingesetzten WLANs untersucht. Dabei wurde festgestellt, dass 44,33% der Funknetze mittels WEP verschlüsselt und 55,67% unverschlüsselt waren.[182] „Wardriver" fahren an Wohn- oder Firmengebäuden vorbei und suchen nach offenen Netzen. Sie bedienen sich einer Software, die in kurzen Intervallen ungeschützte WLANs aufspürt und alle verfügbaren Zugänge übersichtlich anzeigt. Sobald das Gerät ein nicht verschlüsseltes Netz erspäht hat, können die Angreifer in das fremde Netz eindringen.

Tabelle 32: Einschätzung Gefährdungsentwicklung für Mobile Kommunikation

	2007	2009	Prognose
Gefährdungsentwicklung	-	↑	↑

[181] Breitbandstrategie der Bundesregierung, BMWi, Februar 2009, Ziel: Bis 2014 haben 75 Prozent aller Haushalte einen Anschluss mit mind. 50 MBit/s pro Sekunde.

[182] Alexander Gostev, Roel Schouwenberg, Drahtlos auf der CeBIT 2006, www.viruslist.com, 2006

9.2.3 Internet Protocol Version 6 (IPv6)

Das momentan hauptsächlich verwendete Internet Protokoll in der Version 4 (IPv4) wird mittel- und langfristig auf die neuere Version 6 (IPv6) umgestellt. Sämtliche Netzwerk- und Sicherheitsprodukte wie Firewalls, Filter, Router und dergleichen müssen angepasst bzw. neu entwickelt werden. Dies ist momentan noch nicht der Fall, da IPv6 sowohl im Internet als auch in geschlossenen LANs noch nicht weit verbreitet ist. IPv6 wird sich in den kommenden Jahren jedoch durchsetzen, was neue Marktchancen, unter anderem durch neue Produkte und Upgradegeschäft, eröffnet. Allerdings werden auch neue Sicherheitsprobleme bei entsprechenden Implementierungen und Produkten erwartet (z.B. neue Schwachstellen), insbesondere da das Protokoll im Gegensatz zu IPv4 noch nicht im breiten Einsatz erprobt wurde.[183]

Tabelle 33: Einschätzung Gefährdungsentwicklung für IPv6

	2007	2009	Prognose
Gefährdungsentwicklung	-	↑	→

9.2.4 Web 2.0

Web 2.0 Anwendungen wie private Weblogs, Wikis, Social Networks, Bilder- und Video-Portale erfreuen sich zunehmender Beliebtheit. Die für diese Anwendungen notwendigen Technologien wie AJAX oder JavaScript ermöglichen es auch Anwendern mit weniger Techniksachverstand, interaktiv im Internet tätig zu werden. Hierfür müssen Browser speziell freigeschaltet werden, was ein hohes Gefährdungspotenzial eröffnet. Im Halbjahresbericht 2009 des Web Application Security Consortiums (WASC) stellten Angriffe im Zusammenhang mit Web 2.0 mit 19% den größten Anteil an allen in der Web Hacking Incident Database (WHID) erfassten Sicherheitsvorfälle.

Die Gefährdung ergibt sich zum einen durch Anwender, die freiwillig viele personenbezogene Daten ungeschützt ins Internet eingeben und zum anderen durch Angreifer, die in die durch die aktiven Inhalte übertragenen Programmcodes Schadprogramme (siehe 4.4.1.2) einschleusen. Nahezu alle Webseiten weisen entsprechende Schwachstellen auf, die überwiegend für Cross-Site-Scripting-Angriffe ausgenutzt werden. **Cross-Site-Scripting** (XSS) ermög-

[183] Interview mit Herrn Bernhard Schneck, GeNUA GmbH, 2009

licht einem Angreifer unter anderem, Inhalte von Webseiten zu verändern oder Benutzer-Sessions zu übernehmen.[184]

Befragte Unternehmen gaben hierzu an, dass das erhöhte Niveau an Interaktivität und aktiven Inhalten durch Technologien wie AJAX und JavaScript sehr hohe Anforderungen an entsprechende Firewalls stellt. Sollen entsprechende Technologien nicht komplett gesperrt werden, so müssten intelligente Filtermechanismen implementiert werden, die potenziell schadhafte Instruktionen ausfiltern, übrige aktive Inhalte aber passieren lassen. Gartner bezeichnet Web 2.0 als ein Ökosystem einer Reihe weltweit verteilter Anwendungen und Webseiten, das nicht sinnvoll mit einem undurchdringlichen Schutzwall von Firewalls, Intrusion Detection Systems (IDS), Content Filtering, Application Hardening und Data Loss Prevention Systemen versehen werden kann. Die zur Anwendung kommenden Technologien stehen sowohl der friedlichen als auch der kriminellen Nutzung zur Verfügung. Zudem führt die zunehmende Benutzerfreundlichkeit der Entwicklungsumgebung zu einem rasanten Wachstum nicht oder schlecht ausgebildeter Anwendungsentwickler, die keine oder nur geringe Kenntnisse über sichere IT Entwicklung besitzen.

Tabelle 34: Einschätzung Gefährdungsentwicklung für Web 2.0

	2007	2009	Prognose
Gefährdungsentwicklung	-	↑	↑

9.2.5 Cloud Security & Virtualization

Cloud Computing bezeichnet eine Reihe neuartiger Technologien und Anwendungen wie Grid Computing, Utility Computing, Software as a Service (SaaS), Storage in the Cloud und Virtualization. Gut ausgeführt kann eine derartige Verlagerung zu einer Erhöhung des Sicherheitsstandards führen, dessen Einführung und Aufrechterhaltung ansonsten sehr aufwändig sein kann. All diesen Technologien und Diensten ist allerdings auch gemeinsam, dass sie außerhalb des eigenen Netzwerks bereitgestellt werden und die physikalische Speicherung der Firmendaten außerhalb des eigenen Einflussbereichs erfolgt. Experten sehen die Speicherung sensibler Dokumente auf diesen Plattformen außerhalb des Unternehmens daher auch kritisch. Schließlich kann der Anwender zwar seine Sicherheitsanforderungen und rechtlichen Pflichten, ähnlich dem Outsourcing, in Service Level Agreements mit dem

[184] BSI, Die Lage der IT Sicherheit in Deutschland, 2009

Anbieter festlegen, beim Rückgriff auf dessen Sicherheitsvorkehrungen Verfügbarkeit muss er ihm aber letztlich vertrauen können.

Denjenigen, die Cloud Computing und Virtualization als Dienst anbieten, können die Technik für die Netzwerksicherheit physikalisch von den Applikations- und Datenservern trennen. Zudem kann Virtualisierung jeweils nur innerhalb einer der drei Ebenen der Web-Infrastruktur - Web, Anwendung und Daten - erfolgen und angeboten werden und nicht über mehrere Ebenen hinweg.[185]

9.2.6 Radio Frequency Identification (RFID)

Eine Schlüsseltechnologie für viele Einsatzfelder des täglichen Lebens in Wirtschaft und Verwaltung, z.B. im Ticketing bei Sportveranstaltung oder im öffentlichen Personennahverkehr sowie für die Entwicklung des Internets der Dinge, ist die Radio Frequency Identification (RFID) und deren verwandte Identifikationstechnologien. RFID wird eingesetzt zur Identifizierung von Personen, Objekten, Geschäftstransaktionen oder Vorgängen durch drahtlose Kommunikation (Funkverbindung) über elektronische „Etiketten". RFID ist eine automatische Identifizierung und Datenerfassungsmethode, die nicht nur hilft, Dinge und Personen zu identifizieren, sondern in Verbindung mit Sensoren auch bestimmte Merkmale oder Attribute über diese zu sammeln, einschließlich Ortsangaben oder Umgebungsdaten wie Temperatur und Zeit.

Die Europäische Kommission hat in ihrem Fahrplan "Internet of Things in 2020" herausgestellt, dass Vertrauen, Sicherheit und Schutz der Privatsphäre entscheidende Faktoren für die Verbreitung neuer Technologien sind. In der Entwicklung von Sicherheitsmechanismen und -richtlinien liegen hierbei Herausforderungen aber auch Chancen für Anbieter.[186]

In diesem Zusammenhang hat das BSI technische Richtlinien für diverse Anwendungsfelder, z.B. eTicketing und Handelslogistik, erlassen, die dem Anwender der RFID-Technik ein angemessenes Sicherheitsniveau garantieren sollen. Die Richtlinien geben detaillierte Maßnahmen für den sicheren Einsatz der RFID-Technologie in verschiedenen Gebieten vor, z.B. Festlegung des kryptographischen Verfahrens, Schlüsselmanagement und Lese- und Schreibschutzverfahren für RFID-Trägermedium und Transponder, und ermöglichen

---

[185] Throop Wilder, Network World, 2009
[186] The European Network and Information Security Market, IDC EMEA, 2009

nach erfolgreicher Prüfung eine Zertifizierung durch einen unabhängigen Prüfer.[187]

Tabelle 35: Einschätzung Gefährdungsentwicklung für RFID

	2007	2009	Prognose
Gefährdungsentwicklung	→	→	↑

9.2.7 Biometrie

Biometrischen Daten wie z.B. ein Fingerabdruck oder das Muster der Iris im Auge können zur Verbesserung der Zugangs- und Identitätskontrolle gneutzt werden. Neben den hoheitlichen Anwendungsfeldern wie ePass und elektronischer Personalausweis werden zunehmend privatwirtschaftliche Anwendungen wie Zugangskontrollen und Bezahlkarten entwickelt. Auch für das Internet wird an Identifizierungsverfahren mittels Biometrie gearbeitet. Der elektronische Personalausweis wird neben der hoheitlichen Funktion auch eine eID Funktion für kommerzielle Anwendungen enthalten, z.B. de-Mail, bei dem die Bundesregierung gemeinsam mit der deutschen Wirtschaft an einem Dienst für das geschützte und zuverlässige Versenden und Empfangen von elektronischer Post arbeitet.

Allerdings erhöht sich durch die gesteigerte Nutzung biometrischer Daten im Internet mittels eID-Funktion des elektronischen Personalausweises im privatwirtschaftlichen Umfeld die Gefahr verstärkter Angriffe auf die betreffenden Sicherheitsfunktionen.[188] Biometrische Verfahren können auf der einen Seite die Sicherheit im Rechtsverkehr erhöhen, schaffen auf der anderen Seite natürlich auch neue Herausforderungen in Bezug auf den Datenschutz.[189]

Tabelle 36: Einschätzung Gefährdungsentwicklung für Biometrie

	2007	2009	Prognose
Gefährdungsentwicklung	-	↑	↑

9.2.8 Service Oriented Architecture (SOA)

Service Oriented Architectures führen Unterstützungsdienste, die über mehrere IT-Systeme verteilt sind, zusammen, um Geschäftsprozesse abzuwickeln.

---

[187] BSI, Die Lage der IT Sicherheit in Deutschland, 2009
[188] BSI, Die Lage der IT Sicherheit in Deutschland, 2009
[189] Annette Brückner (Intelligents, Gesellschaft für strategische Unternehmensberatung mbH), Sachverständigenanhörung zum neuen BSI Gesetz, Protokoll 16/94 des BT-Innenausschuss, 11.5.2009

Die Sicherheitsanforderungen an SOA-Infrastrukturen sind aufgrund des vertraulichen Charakters sehr hoch. Die Realisierung eines Geschäftsprozesses über eine Vielzahl lose gekoppelter Services erfordert beispielsweise mehr Authentisierungsvorgänge und eine höhere Integrität als über konventionelle Systeme.[23] Eine weltweite Befragung von IT Verantwortlichen durch Computer Associates im Jahr 2008 ergab, dass 93% der Befragten die Integrierung von SOA und Web Services mit den vorhandenen Identitäts- und Zugangsverwaltungssystemen als notwendig erachteten.[190]

Tabelle 37: Einschätzung Gefährdungsentwicklung für SOA

	2007	2009	Prognose
Gefährdungsentwicklung	-	↑	↑

9.2.9 Sonstige

Es gibt bestimmte Technologiebereiche und Anwendungen, die sich nicht in die vorstehend beschriebenen Kategorien eingeordnen lassen. Die nachstehend aufgeführten Technologien bzw. Anwendungen sind durch ihre Funktion bzw. ihrer Funktionalität einem erhöhten Gefährdungspotenzial ausgesetzt sind. Darunter fallen zum Beispiel komplexe Prozesssteuerungssysteme in kritischen Infrastrukturen als auch schlichte USB Schnittstellen, die ein Einfallstor für Schadprogramme sein können.

- **Prozesssteuerungssysteme**

  Prozesssteuerungs- bzw. SCADA (Supervisory Control and Data Acquisition) Systeme werden eingesetzt, um gravierende Unterbrechungen kritischer Infrastrukturen wie beispielsweise die Telekommunikation, das Transportwesen oder auch die Stromversorgung möglichst zu vermeiden. Aus organisatorischen und ökonomischen Gründen werden diese Systeme zunehmend untereinander oder mit anderen Netzen verbunden, was neue sicherheitstechnische Herausforderungen zur Sicherstellung der Verfügbarkeit mit sich bringt.

- **Domain Name System (DNS)**

  Ähnlich der Bedeutung der SCADA Systeme für die kritische Infrastruktur, hat das DNS (Domain Name System) eine Schlüsselrolle beim Funktionieren des World Wide Web. Das DNS sorgt für die Auflösung eines In-

[190] CA Global Survey, Computers, Networks & Communications, 2008

ternet Domain Namens (z.B. www.bund.de) in die tatsächliche IP-Adresse (z.B. 192.178.185.45 (fiktiv)) und hilft so zu vermeiden, dass sich die Nutzer die komplizierten IP-Adressen merken müssen.

Entsprechend seiner Bedeutung ist das DNS einem hohen Gefährdungspotenzial durch Angreifer ausgesetzt, die versuchen in das DNS einzudringen, den Internetverkehr umzuleiten und auf diese Weise persönliche Daten abfangen oder Internetinhalte zu ändern. Zur generellen Verbesserung der Sicherheit des Domain Name Systems wurde in der Fachwelt eine Erweiterung des zugrunde liegenden Protokolls mit dem Namen DNSSEC entwickelt. Dabei stellen kryptographische Verfahren die Authentifizierung und Datenintegrität der DNS-Daten sicher.[191]

- **Multifunktionsgeräte**

  Durch die Integration der Funktionen Scannen, Drucken und Kopieren in einem Gerät steigen die IT-Sicherheitsanforderungen im Vergleich zu einzelnen Systemen, da solche Geräte zusätzlich einen so genannten Single Point of Failure darstellen. Neben dem ungewollten Informationsabfluss aus dem LAN heraus könnte zudem ein netzfähiger Drucker auch unerwünscht Daten aus dem Internet empfangen und eventuell weiterverteilen.

- **Schnittstelle und Speichermedien**

  Insbesondere aufgrund der steigenden Zahl externer Speichermedien wird das Gefahrenpotential das von Schnittstellen ausgeht in Zukunft weiter zunehmen. Laut einer Umfrage im Jahr 2008 sichern 45,5% der Unternehmen ihre Schnittstellen nicht ab bzw. können keine Angaben dazu machen. Als Schnittstellen für einen Datenaustausch mit externen Speichermedien haben sich Firewire und USB (Universal Serial Bus) etabliert. Auf etwa 80 bis 90% der USB-Sticks werden die Daten immer noch unverschlüsselt und ohne Passwortschutz transportiert. Für andere Speichermedien wie zum Beispiel SD-, MMC- oder CF-Speicherkarten ergibt sich eine vergleichbare Problematik.[35]

[191] BSI, Die Lage der IT Sicherheit in Deutschland, 2009

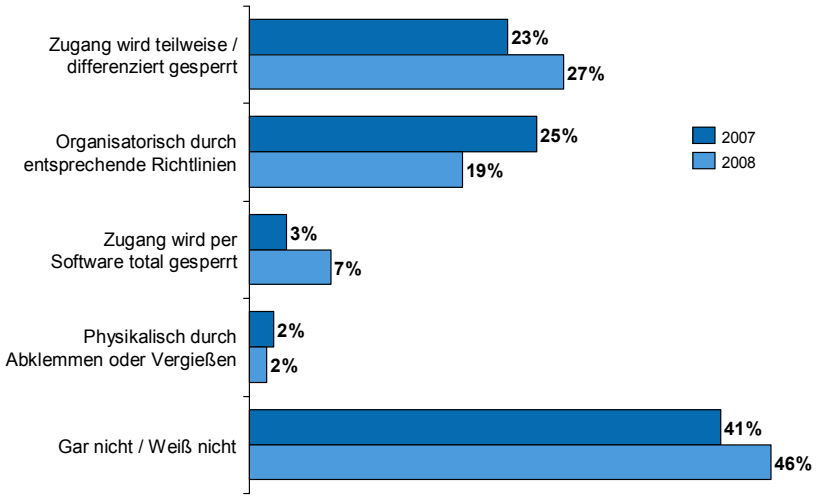


Abbildung 49: Absicherung von externen Schnittstellen (z.B. USB) in deutschen Unternehmen[192]

- **Netzkoppelelemente**

  Angriffe auf Netzkoppelelemente (z.B. Router oder Switches) sind eine ernst zu nehmende Gefahr. Die Anzahl der gemeldeten Schwachstellen in Netzkoppelelementen ist im ersten Halbjahr 2008 im Vergleich zum Vorjahreszeitraum um 61% gestiegen.[193]

  Durch die zunehmende Vernetzung von IT-Systemen sowie der zunehmenden Verbreitung von Breitband-Internetzugängen sind Netzkoppelelemente (Geräte wie Router und Switches) aus Internet und Intranet in Unternehmen, Verwaltung sowie Privathaushalten nicht mehr wegzudenken. Für einen Angreifer stellen solche Knotenpunkte strategische Ziele dar, da nicht nur ein einzelner Rechner angegriffen werden kann, sondern die Kommunikation aller IT-Systeme, die mit dem Netzwerkgerät verbunden sind, manipuliert werden können. Die Gefahr eines Angriffs kann reduziert werden, indem aktuelle und um Schwachstellen bereinigte Betriebssystem- bzw. Firmware-Versionen eingesetzt werden. In Kombination mit sicheren Authentifizierungsmechanismen, der regelmäßigen Auswertung der Protokolldaten von Netzwerkgeräten sowie der Sicherstellung der Betriebssystem- bzw. Firmware-Integrität kann einem Angriff auf Netzkoppelelemente vorgebeugt werden. [194]

- **IT-Sicherheit im Automobil und Verkehr**

[192] InformationWeek, 2009
[193] Securitytracker, http://www.securitytracker.com/topics/topics.html, 2009
[194] BSI, Die Lage der IT Sicherheit in Deutschland, 2009

Elektronische Steuergeräte sowie Computer sind mittlerweile zentraler Bestandteil moderner Fahrzeuge. Ein Fahrzeug verfügt mittlerweile über bis zu 150 Steuergeräte, die über zahlreiche vernetzte Systeme Anwendungsdaten mit unterschiedlichen (Echtzeit)-Anforderungen austauschen. Derartige Funktionen sind auf ein verlässliches Echtzeit-Datennetzwerk mit höchster Verfügbarkeit angewiesen, das zudem wirksam gegen Manipulation geschützt sein muss.