Studie für das BMWi

Industriepolitische Auswirkungen von sicheren IT-Plattformen auf Basis der „Trusted Computing“ (TC) Technologie Projekt Nr. 46/07

Franz Büllingen (WIK-Consult)
Peter Stamm (WIK-Consult)
Annette Hillebrand (WIK-Consult)
Andreas Neumann (IRNIK)

WIK-Consult GmbH
Rhöndorferstr. 68
53604 Bad Honnef

Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie (IRNIK) GbR
Rheinweg 67
53129 Bonn

Bad Honnef, 28. Juli 2008

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ACMDRM	ACM Workshop for Digital Rights Management
ADS	Applied Data Security
AES	Advanced Encryption Standard
AMD	Advanced Micro Devices
BDI	Bundesverband der Deutschen Industrie
BIOS	Basic Input Output System
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
BKA	Bundeskriminalamt
BMWi	Bundesministerium für Wirtschaft und Technologie
BOD	Board of Directors
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAS	China Academy of Sciences
CC	Common Criteria
CCC	Chaos Computer Club
CHES	Cryptographic Hardware and Embedded Systems
CISC	Conference on Information Security and Cryptography
CNITSEC	China Information Technology Security Certification Center
COTS	Commercials of the Shelf
CPU	Central Processing Unit
CRTM	Core Root of Trust for Measurement
CSA	Common Scrambling Algorythm
CTCG	China Trusted Computing Group
DIHT	Deutscher Industrie- und Handelstag
DFG	Deutsche Forschungsgemeinschaft
DFKI	Deutsches Forschungszentrum für Künstliche Intelligenz
DM	Device Management
DOJ	Department of Justice
DRM	Digital Rights Management
DROPS	Dresden Real Time Operating Systems
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECRYPT	European Network of Excellence in Cryptography
EFF	Electronic Frontier Foundation
EFI	Extensible Firmware Interface
EG	Europäische Gemeinschaft
EuG	Europäischer Gerichtshof
EK	Endorsement Key
EMSCB	European Multilaterally Secure Computing Base
ERM	Enterprise Rights Management

eSI	elektronischer Sicherheitsinspektor
ESCAR	Embedded Security in Cars
EU	Europäische Union
F&E	Forschung und Entwicklung
FC	Financial Cryptography
FhG	Frauenhofer Gesellschaft
GMD	Gesellschaft für Mathematik und Datenverarbeitung
GPL	Gnu Public License
GRID	Global Ressource Identifier
GRUB	Grand Unified Bootloader
GSM	Global System for Mobile Communications
GWB	Gesetz gegen Wettbewerbsbeschränkungen
HGI	Horst Görtz Institut
HW	Hardware
ICCSA	Computational Science & Its Application
I/O	Input/Output
IS	Information System
ISEB	Institut für Sicherheit im E-Business
Isits	International School of IT Security
IPR	Intellectual Property Right
ISH	Information Security & Hiding
ISO	Internationale Organisation für Normung
ITK	Informations- und Telekommunikationstechnologie
ITSmiG	IT-Security Made in Germany
ITU	International Telecommunication Union
IWDW	International Workshop on Digital Watermarking
KMU	Kleine und mittelständische Unternehmen
MII	Ministry of Information Industry
MoST	Ministry of Science and Technology
MPEG	Moving Picture Experts Group
MPS	Ministry of Public Security
NAP	Network Access Protection Architecture
NCSD	National Cyber Security Division
NGSCB	Next-Generation Secure Computing Base
NICTA	National ICT Australia
NIST	National Institute of Standard and Technology
NoE	Network of Excellence
NRO	National Reconnaisance Office
NRW	Nord-Rhein-Westfalen
NSPW	New Security Paradigm Workshop
OECD	Organisation for Economic Co-Operation and Development
ONR	Office of Naval Research

OS	Operating System
OSCCA	Office of State Commercial Cipher Administration
OSLO	Open Secure LOader
OSRC	Operating System Research Center
OSS	Open Source Software
PAA	Direct Anonymous Attestation
PC	Personal Computer
PDA	Personal Digital Assistant
PKI	Public-Key-Infrastruktur
PPP	Public Private Partnership
PSE	Personal Security Environment
R&D	Research and Development
RFID	Radio Frequency Identification
ROBIN	Open Robust Infrastructures
RTM	Root of Trust for Measurement
RUB	Ruhr-Universität Bochum
FhGSIT	Fraunhofer Institut für Sichere Informationstechnologie
SFB	Sonderforschungsbereich
SHVT	Simple Homomorphism Verfication Tool
SigG	Signaturgesetz
SPEED	Signal Processing in Encrypted Domain
SSO	Single-Sign-On
STC	Scalable Trusted Computing
STF	Security and Dependability Task Force
SW	Software
SysSec	Lehrstuhl für Systemsicherheit
TC	Trusted Computing
TCG	Trusted Computing Group
TCPA	Trusted Computing Platform Alliance
TCX	Trusted Computing Exemplar
TNC	Trusted Network Connect
TPM	Trusted Platform Module
TSL	Trusted Software Layer
TSS	TCG Software Stack
TUD	Technische Universität Dresden
TÜVIT	Technischer Überwachungsverein Informationstechnologie
TVD	Trusted Virtual Domains
TXT	Trusted Execution Technology
UAC	United Access Control
UEFI	Universal Extensible Firmware Interface
VGV	Vergabeverordnung
VMM	Virtual Machine Monitors

VPN	Virtual Private Network
VT	Virtualization Technology
WATC	Workshop on Advance in Trusted Computing
WeWoRC	Western European Workshop on Research in Cryptology
WISA	International Workshop on Information Security Applilcations

1 Zusammenfassung der Projektergebnisse

Ausgangssituation

Viele Informations- und Kommunikationsprozesse des öffentlichen, wirtschaftlichen und privaten Lebens sind heute ohne Informations- und Telekommunikationstechnologien nicht mehr denkbar. Rund 1,2 Mrd. Menschen nutzen heute das Internet für wirtschaftliche und private Zwecke. Vertraulichkeit, Integrität und Verfügbarkeit bilden daher essentielle Faktoren der Informationsgesellschaft, die zur Aufrechterhaltung von Geschäftsprozessen, beim Transport sowie der Speicherung sensibler Daten unabdingbar geworden sind.

Neben der wachsenden Abhängigkeit unserer Gesellschaft von der Verfügbarkeit der Telekommunikationsinfrastruktur nimmt im Zuge der weltweiten Nutzung des Internet die Bedrohungen durch Malware, Spyware, DoS-Angriffe etc. kontinuierlich zu. Rund 30 neue Viren werden pro Tag über das Internet verbreitet. Der dadurch entstandene Schaden wird alleine für die Unternehmen in den USA auf über 67 Mrd. US$ pro Jahr geschätzt. Das BKA stellt in seinem Bundeslagebild Wirtschaftskriminalität (PKS-Auszug) für das Jahr 2006 fest, dass durch Wirtschaftskriminalitätsdelikte in Deutschland ein Schaden in Höhe von 4,3 Mrd. Euro verursacht wurde.[1]

Nach dem neuesten Bericht des BSI (2007) hat sich die Motivationslage der Angreifer verändert und an die Stelle von Hackern ist die professionalisierte und organisierte Kriminalität getreten. Die Bedrohungslage hat sich hierdurch, aber auch durch die steigende Komplexität der Betriebssysteme, durch Sicherheitslücken in Browsern, durch Java-basierte-Anwendungen sowie durch nomadischen Zugang zu konvergenten Netzen kontinuierlich verschärft. Anforderungen an die IT-Sicherheit und Vertrauenswürdigkeit sind hierdurch deutlich gewachsen.

Die Schaffung einer vertrauenswürdigen Systemumgebung, der Schutz der Hardwareplattformen und die Herstellung sicherer IT-Komponenten stellt somit zweifellos eine der größten Herausforderungen für Hersteller und Anwender dar. Durch die Herstellung eines sicheren physischen Kerns, der sog. „Root of Trust“ soll – bis zu einem gewissen Sicherheitsniveau - der Ansatzpunkt (Anker) für die Etablierung einer Sicherheitskette (Chain of Trust) und dadurch die Voraussetzungen für vertrauenswürdige Anwendungen (Trusted Computing) geschaffen werden. Durch den festen Einbau eines Smart Card-ähnlichen Chips, des sog. Trusted Platform Module (TPM), stehen Funktionalitäten bereit, die sicheres Booten, die Erzeugung kryptografischer Schlüssel, die Verwaltung von Zertifikaten und Referenzwerten, das Signieren von Dokumenten oder die Verifikation von Signaturen ermöglichen sollen. Damit würde eine vertrauenswürdige

---

1 Die mittels Internet in Deutschland begangenen Straftaten werden in der Statistik des Bundeskriminalamtes in der Wirtschaftskriminalität erfasst. Vgl. BKA 2007, S. 3f. Die dort ermittelte Zahl der Fälle verdoppelte sich von 2005 (4.600) bis 2006 (9.700).

Plattform zur Verfügung stehen, von der man weiß, dass sie nicht kompromittiert wurde. Um den Sicherheitsgewinn der durch TPM veränderten Systemarchitektur auszuschöpfen, sind ferner Anpassungen auf der Ebene des Betriebssystems sowie der Anwendungssoftware erforderlich.

Förderinitiativen im Bereich von Trusted Computing

Der EU und insbesondere Deutschland kommt beim Bestreben eines rationalen Umgangs mit Trusted Computing im internationalen Vergleich eine Vorreiterrolle zu. Nach einer sehr kontroversen Diskussion über die wirtschaftlichen und gesellschaftlichen Chancen und Risiken sind in den letzten Jahren eine Reihe einschlägiger F&E-Projekte angestoßen und finanziert worden. Die von der EU bzw. dem BMWi geförderten Projekte wie Open Trusted Computing, ROBIN sowie EMSCB/TURAYA können als wichtige Beiträge betrachtet werden, die Potenziale einer offenen, für alle Anwender verfügbaren und sichereren IT-Plattform auszuloten. Im Rahmen dieser Projekte wurden nach Angaben des Institutes für Internet-Sicherheit (if(is)) Demonstratoren geschaffen, die die Mach- und Umsetzbarkeit von TC-Lösungen dokumentieren sollen. Diese Projekte sind auch deshalb von Bedeutung, weil davon auszugehen ist, dass spätestens bis 2015 alle Endgeräte ein TPM besitzen werden.

Die Bundesregierung zielte in den letzten Jahren darauf ab, die kontroverse Diskussion zu den mit den Standardisierungsaktivitäten des Industriekonsortiums Trusted Computing Group (TCG) verbundenen datenschutzrechtlichen, verbraucherpolitischen, wettbewerbsrechtlichen sowie industriepolitischen Implikationen aufzuhellen und zu versachlichen. Im Rahmen mehrerer Symposien und Workshops wurde eingehend darüber diskutiert, ob die TCG-Standards Open Source-Produkte vom Markt ausschliessen, ob sie Nutzern die Verfügungshoheit über ihre Endgeräte entziehen, ob DRM-restringierende Funktionalitäten eine der Hauptzielsetzungen darstellen oder bestimmte Sicherheitsfunktionen nicht ohne Online-Verbindung genutzt werden können. Allerdings sind manche Einschätzungen bzgl. der Beantwortung einzelner Fragen bis heute kontrovers geblieben.

Ziele und Aufgaben der vorliegenden Untersuchung

Inzwischen wurde insbesondere deutlich, dass das TCG-Konzept noch keineswegs die endgültige Lösung einer Sicherheits-Plattform beinhaltet, sondern dass Entwicklung und Implementierung langwierige Prozesse darstellen, die noch vor der Lösung zahlreicher technischer, institutioneller, innovationspolitischer sowie rechtlicher Hürden stehen. Die Spezifikationsprozesse – und ergebnisse der TCG bilden derzeit lediglich den Rahmen für darauf aufsetzende Lösungen der Hersteller von Betriebssystemen und Anwendungssoftware. Die hierauf basierenden Konzepte sind weder vollständig noch interoperabel und eine entsprechende Endanwender-Software existiert bis dato nicht.

Vor diesem Hintergrund wurde die vorliegende Studie beauftragt mit dem Ziel, eine Analyse des heutigen Standes von Trusted Computing durchzuführen und mögliche Handlungsoptionen auszuloten.

Wichtige Aspekte, die im Rahmen der Studie zu analysieren waren, umfassen die

- Potentiale von TC in der Einschätzungen der Scientific Community, der Verbände, der ITK-Wirtschaft sowie der übrigen Wirtschaft in Deutschland,
- Chancen für die verschiedenen Wirtschaftsbranchen in Deutschland durch die Realisierung von Anwendungen,
- Möglichkeiten und Ansätze einer strategischen Vernetzung der Akteure,
- industriepolitische, wettbewerbspolitische und –rechtliche Risiken von TC,
- Entwicklung und Behandlung von TC in wichtigen ausländischen Vergleichsmärkten,
- Szenarien zur zukünftigen Entwicklung und Anwendung von TC.

Durchführung der Studie und Methodik

Die Studie wurde von Juli 2007 bis Dezember 2007 durchgeführt. Im März 2008 wurden nach der Kommentierung durch den Auftraggeber wichtige Veränderungen und Ergänzungen vorgenommen. Im Juli 2008 wurden nach enstprechenden Recherchen weitere Ergänzungen und Veränderungen vorgenommen.

Die Studie basiert zum einen auf einer systematischen Auswertung und Analyse der öffentlich verfügbaren Sekundärquellen sowie der Online-Recherche. Im Literaturteil wurden nur solche aus dem Internet verfügbaren Quellen zitiert, von denen zu erwarten ist, dass sie auch längerfristig in unveränderter Form verfügbar bleiben. Andere Quellen aus dem Internet wurden jeweils in den Fußnoten zitiert.

Zum zweiten wurden im Rahmen der Studie mehr als zwei Dutzend Expertengespräche durchgeführt. Die Experten stammen aus dem Bereich der Wissenschaft (einschließlich F&E), der Wirtschaft, der Verbänden sowie der öffentlichen Verwaltung und wurden vorab mit dem Auftraggeber abgestimmt. Methodisch basierten diese Gespräche auf einem strukturierten Leitfaden (s. Anhang), der ebenfalls vorab abgestimmt wurde. Angesichts der qualitativ ausgerichteten Studie wurde dieses explorative Verfahren gewählt, um die seit 2004 stark verschlechterte Quellenlage zu kompensieren und um einen möglichst aktuellen Stand der Einschätzungen zu TC dokumentieren zu können. Die Durchführung der Gespräche erfolgte in der Regel in Face-to-Face-Interviews, so dass alle Fragen und Antworten eingehend diskutiert werden konnten. Bzgl. der Aussagen wurde generell um die Wahrung der Anonymität und der Vertraulichkeit gebeten.

Die (Zwischen-)Ergebnisse wurden auf einem internen Workshop des BMWi am 29. Oktober 2007 in Bonn sowie einer Arbeitsgruppenveranstaltung des BITKOM am 4. Dezember in Frankfurt vorgestellt und diskutiert.

Wichtigste Ergebnisse

Deutschland gehört nach allgemeiner Einschätzung der Experten zu den im Bereich TC führenden Nationen. Die F&E-Kapazitäten sind im Wesentlichen auf drei Hochschulen sowie ein Forschungs- und Beratungsinstitut konzentriert, an denen zwischen 80 bis 150 Experten mit TC befasst sind. Daneben gibt es eine Reihe von Firmen, die im Bereich der IT-Sicherheit als Anbieter von Produkten und Dienstleistungen aktiv sind und die teilweise auch in der TCG mitarbeiten. Aus Sicht von F&E besteht zum einen die Notwendigkeit, Grundlagenaspekte im Bereich der verschiedenen Technologien TC, Mikrokernentwicklung sowie Virtualisierung zu vertiefen und zu marktreifen Lösungen zu entwickeln.[2] Auf der anderen Seite wird die Notwendigkeit betont, den Transfer von Know-how in die industriellen Anwendungsbereiche zu organisieren und zu verstärken.

Bislang steht dieser Austausch zwischen Forschung und Anwendung auf noch schwachen Beinen und das Interesse an TC beschränkt sich im Wesentlichen auf einzelne Branchen wie z. B. die Automobilindustrie. Vor diesem Hintergrund verwundert es nicht, dass die Awareness bzgl. der industriepolitischen Chancen von TC insbesondere in den übrigen Wirtschaftssektoren und in der Verwaltung noch wenig ausgeprägt ist. Ein großer Teil der wissenschaftlichen Akteure stimmt darin überein, dass TC eine strategische Entwicklung darstellt, um wachsenden Bedrohungen der IT-Sicherheit zu begegnen und Prozesse insgesamt sicherer zu gestalten. Ein anderer Teil vertritt allerdings auch die Auffassung, dass bereits eine Reihe von bewährten Sicherheitstechnologien zur Verfügung stehen, die alternativ oder ergänzend zu TC genutzt werden können.

Die im Rahmen dieser Studie ausgewerteten Dokumente, die zahlreichen Gespräche mit IT-Sicherheitsexperten sowie die Analysen der Vergleichsmärkte legen auf der einen Seite den Schluss nahe, dass es sich bei Trusted Computing insbesondere bei Embedded Systems um eine Schlüsseltechnologie handelt, die es allen Systemherstellern erlaubt, bei der Entwicklung die gegenwärtigen Komplexitätsschranken und Bedrohungen zu überwinden. Es können mit ihrer Hilfe Netzwerke, Plattformen, implementierte Systeme und Endgeräte entwickelt werden, die eine sich immer stärker vernetzende industrielle Gesellschaft benötigt, um das erforderliche Vertrauen in alle Formen von Austauschprozessen und Transaktionen herzustellen.

---

2 Grundsätzlich stellen Trusted Computing, Mikrokerne und Virtualisierung unabhängige Technologien zur Erhöhung der IT-Sicherheit dar, die sowohl einzeln als auch in beliebiger Kombination eingesetzt werden können. Im Rahmen der durchgeführten Expertengespräche wurde deutlich, dass der Begriff Trusted Computing häufig synonym für den Einsatz eines oder mehrerer Verfahren verwendet wird. Das Projekt EMSCB beispielsweise greift auf alle drei Technologien zurück, wird aber meist unter dem Stichwort Trusted Computing vermarktet.

Während allerdings noch vor wenigen Jahren ein weit verbreiteter Optimismus vorherrschte, dass eine Trusted Computing-Architektur eine hinreichend vertrauenswürdige Systemumgebung für alle Betriebssysteme und Arten von Anwendungen bereitstellen würde, gilt inzwischen als allgemein akzeptiert, dass eine „sichere“ Hardware und die auf ihr basierenden Funktionalitäten und Prozesse nur dann faktisch den gewünschten Sicherheitszugewinn bereitstellen können, wenn zugleich auch die darauf aufsetzenden Betriebssysteme sicherer gemacht werden.

Nicht zuletzt auf Grund dieser Tatsache ist die Entschlossenheit, entsprechend (risikobehaftete) Investitionen zu tätigen bzw. mit pilotierten Anwendungen Erfahrungen zu sammeln, bislang noch sehr gering ausgeprägt. Es ist nicht zu übersehen, dass es bislang an wirklich sichtbaren oder relevanten industriellen Anwendungen und deren Umsetzung mangelt und niemand Angaben darüber machen kann, in welchen Bereichen sich TC zuerst in mittel- oder langfristiger Perspektive durchsetzen wird. Dieser Umstand erschwert die Schaffung einer breiten Awareness für die Chancen von TC in den Anwenderbranchen. Es betsteht der Eindruck, dass diese Technologie der massenmarktlichen Verbreitung noch weit vorauseilt.

Zusammengefasst bedeutet dies, dass das hohe Maß an Unsicherheit, dass die TC-Entwicklung in den vergangenen Jahren, meist umschrieben mit dem Begriff der „Janus-Köpfigkeit“, mittelfristig fortbestehen wird. Dies muss jedoch für alle Akteure und Entscheidungsträger aus dem forscherischen, wirtschaftlichen sowie politischen Umfeld als in hohem Maße unbefriedigend empfunden werden. Auf der einen Seite gilt es zu vermeiden, dass durch ein voreiliges Handeln auf der Basis unvollständiger Informationen knappe Mittel und Ressourcen fehlalloziert werden. Auf der anderen Seite gilt es ebenso zu verhindern, dass sich Deutschland, wie teilweise schon in der Vergangenheit, als Vorreiter im Besitz einer wichtigen Technologie mit Schlüsselcharakter befindet, deren Sicherheits- und Wirtschaftspotenziale auf Grund einer allzu großen Zögerlichkeit verschenkt und den Unternehmen anderer Ländern zur Vermarktung überlassen werden.

Entwicklungsszenarien und Handlungsoptionen zu Trusted Computing

Um diese Unsicherheiten zu reduzieren, wurden im Rahmen dieser Studie ein „Trendszenario“, ein „Wachstumsszenario“ sowie ein „Stillstand-Szenario“ entwickelt, deren Zeithorizont bis zum Jahr 2013 reicht. Das Trendszenario ist das mit der höchsten Eintrittswahrscheinlichkeit. Allerdings besitzt auch eine Mischung von „Trendszenario„ und „Stillstand-Szenario“ eine große Eintrittswahrscheinlichkeit, während das „Wachstumsszenario“ wenig wahrscheinlich ist.

Für jedes dieser Szenarien wurden Handlungsoptionen konzipiert, die möglichst passgenau auf den in der vorangegangenen Analyse skizzierten Entwicklungen aufsetzen. Die auf diesen Szenarien aufsetzenden unterschiedlichen Handlungsperspektiven legen nahe – mit abgestufter Intensität – folgende Optionen zu prüfen:

- ein mehr oder minder intensives Monitoring der nationalen und internationalen TC-Entwicklung sowie der unterschiedlichen Akteursstrategien der nächsten Jahre,

- die Entwicklung einer unterschiedlich akzentuierten Roadmap im Bereich der TC-Grundlagenforschung insbesondere in Hinblick auf die Weiterentwicklung von Mikrokernen sowie Virtualisierungsstrategien,

- die Sicherung des Know-how-Vorsprungs im Bereich der Grundlagenforschung, im Bereich Forschung&Entwicklung sowie bei der Ausbildung durch Vergabe von öffentlichen F&E-Mitteln,

- Identifikation der Ansätze und Intensivierung der Aktvitäten für den Technologie-Transfer von Demonstratoren hin zur breiten industriellen Anwendung,

- Auslotung von Anwendungsmöglichkeiten der TC-Technologie etwa im Rahmen von Public Private Partnerships in der öffentlichen Verwaltung,

- Gespräche mit einzelnen, besonders IT-Sicherheits-sensitiven Branchen wie etwa Banken, Versicherungen oder Technologieträgern,

- Entwicklung einer Strategie der aktiven Vernetzung und verbesserten Kommunikation der Akteure etwa im Rahmen einer erweiterten Arbeitsplattform beim Branchenverband TeleTrusT, sowie

- die Schaffung von Awareness in den Anwenderbranchen durch unterschiedliche Medien (z. B. Broschüren zum State-of-the-Art) und Kommunikationsprozesse (Fokusgruppen, branchenbezogene Workshops) mit Hilfe der Branchenverbände.

Wettbewerbspolitische Implikationen

In den dynamischen und komplexen IT-Märkten ist der funktionsfähige Wettbewerb besonderen Gefahren ausgesetzt. Dies wird gerade auch an den zwar zahlenmäßig geringen, aber z. T. grundlegenden Verfahren deutlich, die von der Kommission seit 1980 in diesem Wirtschaftsbereich geführt wurden. Dennoch fehlt es an Hinweisen darauf, dass die Marktteilnehmer innerhalb und außerhalb der TCG bei der Entwicklung der Trusted Computing-Technologie tatsächlich entsprechende Wettbewerbsrisiken sehen. Dabei ist unklar, ob solche Wettbewerbsgefahren bewusst verschwiegen werden, ob ihre Wahrnehmung von der Aussicht auf die wettbewerblichen Chancen des Trusted Computing überlagert wird, oder ob es sie tatsächlich nicht gibt.

Letzteres stünde in einem kaum erklärbaren Widerspruch zu den Erkenntnissen aus anderen IT-Märkten. Die theoretische Literatur hat demzufolge auch mehrere potenzielle Wettbewerbsbeschränkungen identifiziert. So werden auf Ebene der Standardisie-

rung diskriminierende Effekte zulasten kleiner und mittlerer Unternehmen durch die Ausgestaltung der Mitgliedschaft in der TCG, uneinholbare Wettbewerbsvorsprünge der Gründungsmitglieder und die Gefahr der Steuerung des Spezifikationsprozesses durch Microsoft thematisiert. Gegenüber dieser Position kann geltend gemacht werden, dass große Unternehmen innerhalb der TCG einen großen Einfluss verfügen, gleichzeitig aber auch divergierende Interessen verfolgen. Wie Standardiserungsprozesse aus anderen Branchen zeigen, impliziert dies, dass Spezifikationen häufig gebremst und Kompromisse oft auf der Basis eines kleinsten gemeinsamen Nenners geschlossen werden. Die Mitgliedschaft vieler Großunternehmen kann also durchaus zu einem Gleichgewicht der Kräfte führen und geht keineswegs automatisch zu Lasten von KMU.

Daneben werden wettbewerbspolitische Gefahren bei der Gestaltung eines Trusted Computing-Betriebssystems durch ein marktbeherrschendes und vertikal integriertes Softwareunternehmen gesehen: Hier drohen Zugangsbeschränkungen hinsichtlich notwendiger Schnittstelleninformationen, durch die die bestehende Marktmacht mit Hilfe der DRM-Funktionalitäten von Trusted Computing sogar auf nachgelagerte Inhalte- und Dienstemärkte ausgedehnt werden könnte. Außerdem könnte der Wettbewerb auf nachgelagerten Trusted Computing-Applikationsmärkten (für Sicherheitssoftware, Virenschutzprogramme etc.) durch die Kopplung entsprechender Komponenten an ein marktdominantes Betriebssystem beschränkt werden. Nicht ausgeschlossen sind auch Wettbewerbsbeschränkungen durch die Verweigerung von Lizenzen für notwendige Trusted Computing-Technologiekomponenten zu angemessenen Bedingungen sowie im Rahmen entsprechender Lizenzvereinbarungen.

Die Verhinderung von Wettbewerbsgefahren ist zuvörderst die Aufgabe des Wettbewerbsrechts selbst. Dessen unmittelbare Steuerungswirkung kann über den Erlass von Leitlinien und Auslegungshinweisen durch die zuständigen Wettbewerbsbehörden erheblich gesteigert werden. Das gilt gerade auch angesichts der wettbewerbsrechtlichen Risiken, die im Falle von Trusted Computing einen erheblichen Komplexitätsgrad aufweisen.

Wo die Steuerungswirkung des Wettbewerbsrechts alleine nicht ausreicht, kann es erforderlich werden, dass die zuständige Wettbewerbsbehörde zum Schutz des Wettbewerbs ein entsprechendes Verfahren einleitet. Ermittlungsmaßnahmen im Rahmen eines solchen Verfahrens setzen voraus, dass tatsächliche Umstände auf eine Verletzung des Wettbewerbsrechts hindeuten. In Betracht kommen aber auch Enqueteuntersuchungen eines ganzen Wirtschaftsbereiches, die bereits dann möglich sind, wenn bestimmte Umstände vermuten lassen, dass der Wettbewerb möglicherweise beschränkt ist.

Im Rahmen eines konkreten Kartell- oder Missbrauchsverfahrens können noch vor Verfahrensabschluss einstweilige Maßnahmen getroffen werden. Solche Maßnahmen werden im Falle von Trusted Computing jedoch voraussichtlich nur ausnahmsweise in Betracht kommen. Grund hierfür ist gerade die Komplexität der dort zu erwartenden Fra-

gen. Diese wird einer frühzeitigen Substantiierung entsprechender wettbewerbsrechtlicher Bedenken oftmals entgegenstehen. Diese Komplexität hat auch zur Folge, dass endgültige Abhilfemaßnahmen in aller Regel erst nach Abschluss langjähriger Ermittlungsverfahren ergehen können. Dies deckt sich mit den Erfahrungen aus der wettbewerbsrechtlichen Praxis und wirft die generelle Frage nach der Wirksamkeit des allgemeinen Wettbewerbsrechts in IT-Märkten auf. Sollte es im Bereich des Trusted Computing zu Ermittlungen der Wettbewerbsbehörden kommen, erscheint vor diesem Hintergrund eine möglichst frühzeitige Verfahrensbeilegung durch entsprechende Verhaltenszusagen als praktisch sinnvolle Alternative. Voraussetzung hierfür ist indes eine entsprechende Kooperationsbereitschaft des betreffenden Unternehmens.

Ein möglichst frühzeitiger Schutz des Wettbewerbs kann jenseits des Wettbewerbsrechts möglicherweise auch durch staatliches Informationshandeln erreicht werden. Maßgeblich ist hierfür die einschlägige Rechtsprechung des Bundesverfassungsgerichts, die allerdings sehr umstritten ist. Auf ihrer Grundlage dürfte eine entsprechende Informationstätigkeit hinsichtlich ernstzunehmender Wettbewerbsgefahren im Zusammenhang mit der Trusted Computing-Technologie in den Aufgaben- und Zuständigkeitsbereich der Regierung bzw. des Bundeswirtschaftsministers fallen. Solche Informationen müssen aber inhaltlich zutreffend sein und unter Beachtung des Gebots der Sachlichkeit und mit angemessener Zurückhaltung formuliert werden. Vor allem aber dürfen sie kein funktionales Äquivalent eines Grundrechtseingriffes sein.

Es spricht daher viel dafür, von der Möglichkeit staatlicher Informationstätigkeit im Bereich des Trusted Computing, wenn überhaupt, nur sehr zurückhaltend Gebrauch zu machen. Zu denken wäre evtl. noch daran, über drohende Wettbewerbsgefahren im Vorfeld tatsächlicher Wettbewerbsbeschränkungen zu informieren. Auch auf wettbewerbspolitisch unerwünschte Entwicklungen, die außerhalb des Anwendungsbereiches der wettbewerbsrechtlichen Verbotsnormen liegen, könnte staatlicherseits evtl. informiert werden. Das betrifft beispielsweise die volkswirtschaftlichen Konsequenzen weitgehender Pfadabhängigkeiten, die durch Trusted Computing geschaffen bzw. verstärkt werden können.

Konkret marktregulierenden Einfluss kann der Staat auch im Rahmen seiner Beschaffungstätigkeit nehmen. Dieser kann indes nur punktuelle Steuerungswirkung entfalten, da insoweit umfassende rechtliche Vorgaben bestehen, die den Beschaffungsvorgang grundsätzlich an reinen Wirtschaftlichkeitserwägungen ausrichten. Das staatliche Beschaffungswesen wird daher nicht geeignet sein, grundlegende wettbewerbliche Fehlentwicklungen zu korrigieren. Es kann allerdings dazu beitragen, der Verwirklichung einzelner wettbewerbspolitischer Risiken entgegenzuwirken. Insoweit ist auch die von entsprechenden Anforderungen ausgehende Signalwirkung zu berücksichtigen.

Angesichts der potentiellen Wettbewerbsgefahren im Bereich des Trusted Computing ließe sich vor allem daran denken, bestimmte Interoperabilitätsanforderungen als Leistungsanforderungen für die zu beschaffenden IT-Produkte vorzugeben. Entsprechende

Anforderungen an die Interoperabilität und die Unterstützung offener Dateiformate könnten aber auch im Rahmen von Zuschlagskriterien Berücksichtigung finden, da sie i. d. R. auch mit wirtschaftlichen Vorteilen für den staatlichen Auftraggeber verbunden sein werden. Schlussendlich könnte auch durch Vorgaben für die Ausführung des Beschaffungsauftrages auf einzelne wettbewerbspolitische Risiken des Trusted Computing reagiert werden. So könnte z. B. sichergestellt werden, dass etwaige Trusted Computing-Komponenten deaktiviert ausgeliefert werden. Auch könnte auf diese Weise verlangt werden, dass Trusted Computing-spezifische Betriebssystemerweiterungen, zu denen es alternative Programme von Seiten anderer Anbieter gibt, bei der Auslieferung des beschafften Betriebssystems nicht als voreingestellte Lösungen vorgegeben werden.

Wettbewerbsrechtliche Handlungsempfehlung

In den ersten Jahren der TCG führte aus wettbewerbspolitischer Sicht die Ausgestaltung der Mitgliedschaft zu einer Diskriminierung kleiner und mittlerer Unternehmen. Seither wurden die Mitgliedsbeiträge deutlich gesenkt und dadurch das Diskriminierungspotenzial abgebaut. Für einen Jahresbeitrag von 16.500 US$ kann heute jedes KMU innerhalb der TCG den „Contributor“-Status einnehmen. Zudem könnten KMU durch ein stärkeres Engagement der Verbände in den entsprechenden Gremien besser repräsentiert werden. Nicht zuletzt das Engagement des BSI innerhalb der TCG bildet eine gewisse Garantie dafür, dass die freien Entwickler sowie deutsche Firmen Zugang zu den Ergebnissen und dem Know-how der TCG haben.

Für die Vermeidung künftiger Wettbewerbsbeschränkungen empfiehlt es sich demgegenüber, die Märkte durch den kombinierten Einsatz verschiedener Steuerungsinstrumente offen zu halten. Zu denken ist an die Veröffentlichung von Leitlinien und Auslegungshinweisen der Wettbewerbsbehörden zur Anwendung des Wettbewerbsrechts in den IT-Märkten, die Erarbeitung übergreifender Grundsätze für die Berücksichtigung von Interoperabilitätsanforderungen und offenen Dateiformaten bei der staatlichen IT-Beschaffung und ggf. auch an staatliche Informationstätigkeit zum Trusted Computing, etwa durch die Aktualisierung der Stellungnahme der Bundesregierung zu TCG und NGSCB aus dem Jahr 2004.

Daneben sollten schon jetzt die notwendigen Vorkehrungen dafür getroffen werden, dass bei Anzeichen für eine tatsächliche Wettbewerbsbeschränkung unverzüglich entsprechende Wettbewerbsverfahren eingeleitet werden können.

2 Management Summary

Present situation

Nowadays most information and communication processes in public, economic and private life are based on information and telecommunication infrastructure. More than 1.2 bn people worldwide are on the internet making use of this global medium for their private and business purposes as a matter of course. Confidentiality, integrity and reliability are therefore regarded to be basic factors in information society being absolutely essential for the maintenance of business processes, for the transportation as well as the storage of sensible data.

Beside the extending dependability of our society on telecommunication infrastructur, the occurring treats by malware, spyware, viruses, denial-of-service attacks etc. increase continuously. More than 30 new viruses spread over the internet per day. The related costs caused by internet based attacks on enterprises in the US are estimated to exceed 67 bn US$ per year. Germany's Federal Criminal Police Office (BKA) indicates in its latest report on national criminal incidents for 2006 that the costs induced by internet crime amount up to 4.3 bn Euro for 2006 only.

According to one of the latest reports of the Federal Office for Information Security (BSI), the motivation of internet attackers has altered and hackers have been more or less replaced by organised and professional crime. The state of threats has aggravated not only by the growing complexity of operating systems, by security flaws of internet browsers and by Java-based applications but also by ubiquitious nomadic access to the internet over convergent networks. Therefore requirements regarding IT-security as well as the reliability of devices and infrastructure have increased strongly.

The creation and implementation of reliable IT systems, the protection of hardware-platforms and the production of secure IT components impose a major challenge on manufacturer and adopter. By means of a secure physical platform, the so called “root of trust”, an anchor should be implemented as a starting point to establish a chain of trust. This architecture is regarded by experts to provide the necessary prerequisites for secure and trustable computing. Integrating or fixing a so called Trusted Platform Module (TPM) on the motherboard, such a modul provides functionalities like secure booting, creation of cryptografic keys, maintenance of certificates, signing of documents, or the verification of digital signatures. Using these means a user should be assured that a platform has not been compromised. To reap the full benefits of Trusted Computing (TC) changes of the operating systems and applications should be adopted.

Political initiatives promoting Trusted Computing

The European Commission (EC) and the German Ministry of Economics and Technology (BMWi) are outriders to promote rational tackling of TC. After a strong and controversial debate on TC until 2004 about the economic and societal chances and risks, a couple of R&D projects have been raised in recent years. Open Trusted Computing (OTC), ROBIN and EMSCB represent such projects which have been financed by the Comission or the BMWi. These projects can be regarded as most important activities worldwide to level out the potencial economic and societal advantages of secure computing platforms. In the context of EMSCB for instance so called “demonstrators” have been worked out to give prove of the principle feasibility and applicability of TC solutions according to the Institut für Internet-Sicherheit (if(is)). Moreover these projects are most important regarding the fact, that most computing platforms will contain a TPM by 2015.

In the last years the German Government`s policies aimed at settling the controverse discussion on the activities of the Trusted Computing Group (TCG). Several workshops have been organised providing more information about related impacts on data protection, consumer protection, competition law and industrial politics. In theses discussions it could be proved that the TCG standards neither suppress Open Source products, nor impose restrictions on the power and selfdetermination of users, that they constrain the right of freely using of digital goods and that remote attestation functionalities can only be used being connected to the internet.

Purpose of the study

In recent years it has become obvious, that the TCG activities will not provide the ultimate solution for secure computing, but that the development and the implementation of TC constitute a livelong process and numorous technical, institutional, industrial and jurisdictional barriers have to be beared down. Keeping this background in mind the present study has been issued by the BMWi in order to analyse the status quo of TC and to examine potential political options.

The most important aspects comprise

- the assessment of TC by the Scientific Community, the industry associations, ICT-enterprises and industrial appliers,
- the assessment of the potential economic advantages for different industrial branches,
- the analysis of possibilities and strategies to create social networks among all relevant actors,
- the assessment of (potential) impacts of TC on industry, competition and law,

- the analysis of TC-related activities in industrialised countries such as China and the USA,
- the writing of different scenarios describing and forecasting plausible development trends in TC and their impacts on industry and society.

The study has been carried out from July until December 2007. It is based on the systematic evaluation of secondary sources and materials as well as on numorous structured in-depth-interviews. The (interim) results have been presented and discussed at an internal workshop of the BMWi and at a meeting of the IT-security working group of the ITC-industry association BITKOM.

Main results

According to the interviewed experts, Germany is one of the leading countries in the field of TC. Its expertise is concentrated on three universities and one R&D-institute, employing between 80 and 150 TC-experts. Aside several small and medium enterprises are engaged in TC being active suppliers of ITC-related goods and services. Partially they have also joined the TCGs work. From the Scientific Communities view it seems to be necessary to intensify R&D in the area of microkernel development and virtualisation techniques. On the other hand they claim the necessity of technology transfer in order to come to solutions ready to be sold to the mass market.

So far the exchange between the Scientific Community and industry has been weak and there are only a few branches being interested in TC like for instance the automobile industry. Unsuprisingly the awareness of the industrial and societal chances of TC is not very pronounced in most other industry sectors and public institutions. Nevertheless, the Scientific Community is convinced of the strategic importance of TC underlining unmistakingly the growth of threats induced by the internet. Industrial actors meanwhile pinpoint the relevance of TC being embedded in most devices using computing power. As a result most of the experts stress the enormous potential importance of TC as a key solution and a strategic factor for Germany as a business location.

Amalgamating and condensing the evidence of TC related documents, expert interviews and the results of the international comparison of TC adopting countries it can be concluded, that TC – especially Embedded Systems - can be regarded as a key technology enabling suppliers to creat barriers and platforms against the growing challenges towards information society. TC and Embedded Systems provide the technical means to implement secure networks, platforms, and (mobile) devices to manage systems which are necessary to create trust for any kind of electronic information exchange and transactions.

Furthermore it has to be outlined, that TC-related activities in industry and the readiness to invest in R&D is still at the beginning. So far there is still a lag of visible and convinc-

ing applications and no one of the interviewes seems to be able to assess or predict the real meaning of TC for the marketing of IT products or services in the middle or long term. This imponderability seems to impose heavy burdens on creating more awareness of TC in industry. It seems like if the development of TC is far ahead of relevance for mass market products and services.

Summarising these conclusions, it has to be outlined that the imponderabilities adressing the development of TC will subsist within the next years. All questions aiming at more information and distinctiveness about the “Janus-faced” ambiguity (chances and risks) will only be answered in the long term which is regarded to be dissatisfying for most actors. On the one hand, hasty conclusions regarding the allocation of ressources for R&D projects or products have to be avoided because of the risk of sunk investments. On the other hand one has to be aware of the fact that key technologies should not be left for benefitting foreign actors and their market aktivities like it has happened to German inventors for several times in the past.

Szenarios and policy options

In order to reduce TC uncertainties three szenarios have been written comprising a “best case szenario”, a “worst case szenario” and a “trend szenario” reaching until the year 2013 in order not to be to speculative. We expect the “trend szenario” to be the most propable one. Each of these scenarios contains policy options closely based on the findings of the recent study and recommend the following:

- Implementation of a monitoring process of national and international developments of TC watching closely the strategies of relevant actors and their R&D and marketing activities,
- Development of a national “TC-Roadmap” in order to indentify and concretise the necessities in R&D with special regard to the area microkernel and virtualisation techniques,
- Safeguarding the advantages of TC knowledge in the area of basic research, R&D as well as in education and training,
- Intensification of activities promoting technology transfer in order to enable mass market penetration,
- Identification of areas to adopt TC related solutions in the context of public institutions such as eGovernment based e.g. on Public Private Partnerships,
- Organisation of workshops in order to rise awareness and to discuss the potentials of TC in IT security sensitive areas like banks, ensurances or highly innovative technology branches,

- Development and implementation of a strategy creating social networks and platforms improving communication between all actors by being supported by the branch association TeleTrusT,

- Improving awareness by creating and distributiong different media and by conducting workshops or focus groups with representatives of all potential adopter branches.

Implications for Competition Policy

Workable competition faces many dangers in the IT markets with their dynamic and complex environment. This has found expression in the few, but partly fundamental investigations that have been carried out by the Commission of the EC since 1980 in this industry sector. Nonetheless, there is no indication that market participants inside and outside of the TCG actually have identified such risks for competition in the context of the development of Trusted Computing technology. It is not certain, whether such risks are concealed, whether they are overlooked in view of the competitive prospects of Trusted Computing, or whether they simply do not exist.

The last-mentioned option would be contradictory to the experiences of other IT markets and thus hardly explainable. In fact, academic literature has identified several potential risks for unrestricted competition. Concerning the standardisation process, discriminatory effects on small and medium-sized companies have been identified with regard to the terms of membership in the TCG as well as not recompensable advantages for the founder members of the organisation and the risk of a dominant influence of Microsoft on the standardisation process.

Furthermore, potential risks for competition are seen in the context of a Trusted Computing operating system developed by a dominant and vertically integrated software company: Such a company would have incentives and possibilities to restrict access to essential interface information and to extend its market power by means of the DRM funcionality of Trusted Computing even to downstream markets for content and services.

Moreover, competition on downstream markets for Trusted Computing applications (e. g. security or antivirus software) could be hampered by coupling respective components with a dominant operating system. Finally, it seems not to be impossible that competition may also be restricted by refusing to grant licenses for essential components of Trusted Computing technology on fair and reasonable terms or within respective license agreements.

The prevention of risks for competition is first and foremost the task of competition law itself. The immediate effect on the behaviour of the market participants caused by competition law can be significantly increased by means of guidelines and interpreting notes

published by the competent antitrust authorities. This especially applies to the risks for competition in the case of Trusted Computing, since they show a rather high degree of complexity.

Where this immediate effect of competition law alone is not enough, it might be necessary that a procedure is opened by the competent antitrust authority to protect competition. Investigative measures within such a procedure require that the actual circumstances indicate a violation of competition law. Additionally, the antitrust authorities might carry out a sector inquiry, which is already possible when circumstances suggest that competition may be restricted or distorted.

Within a procedure concerning an illegal cartel or the abuse of a dominant position, the antitrust authority may take interim measures even before the investigations have come to an end. In the case of Trusted Computing, however, such measures probably will only be possible in exceptional circumstances. This is due to the high complexity of the questions which will probably arise in such a case and which will not allow to substantiate concerns regarding competition law at an early stage of the respective procedure.

With regard to this complexity, final remedies can probably be imposed only after many years of prior investigations. This prediction is in line with the experiences from the practical application of competition law and raises the fundamental question whether general competition law is sufficiently effective with regard to IT markets. Against this background, it seems to be an appropriate alternative to come to an early settlement based on respective commitments of the undertaking in question, if antitrust authorities will have to act in the field of Trusted Computing. This, however, requires that the undertaking concerned is willing to offer such a commitment.

Beyond competition law, competition might also be protected at an early stage by means of public information policy. The legal standards for such policy are set by the relevant case law of the German Federal Constitutional Court, which is, however, highly controversial. Based on this case law, publishing information about serious risks for competition in the field of Trusted Computing should fall under the tasks and competencies of the Federal Government, respectively of the Federal Minister of Economics. Information published must be correct and expressed in an objective and restrained manner. Furthermore, such information policy must not be the functional equivalent of an intended restriction of a fundamental right like it can be seen in an administrative measure against certain companies.

Against this background, it seems recommendable to make use of public information policy in the field of Trusted Computing only very reluctantly, if at all. A possible example for public information might apply to potential risks for competition in the forefront of actual restrictions of competition. Public information might also be possible with regard to undesirable developments beyond the competition law's scope of application. This

might comprise, inter alia, the economic consequences of extensive path dependencies that could be caused or strengthen via Trusted Computing.

Furthermore, public authorities may take regulating influence on the markets by means of their procurement activities as well. Such influence, however, can only take a punctual effect because of the far-reaching legal requirements that focus public procurement, in principle, on pure economic efficiency. Public procurement, therefore, will not be able to adjust fundamental problems with regard to competition policy. However, public procurement can help to prevent that certain competitive risks actually take effect in practice. In this context, corresponding requirements may also have a considerable impact on the public opinion.

With regard to the potential dangers for competition in the field of Trusted Computing, it might be particularly possible to define certain interoperability requirements as technical specifications for IT products subject to a procurement procedure. Respective requirements regarding interoperability and support of open file formats might also be taken into account as selection criteria, as they usually involve economic benefits for the contracting authority. Finally, it could be possible to take care of certain risks of Trusted Computing for competition by defining requirements on the execution of the respective contract. Such requirements may include the obligation to deactive Trusted Computing components before delivery. They may also be used to make sure that Trusted Computing components of an operating system are not preset within the purchased operating system if other software companies offer competing solutions for such components.

Competition Policy Recommendations

From a competition policy point of view, the terms of membership in the TCG lead to an ongoing discrimination of small and medium-sized companies. To prevent future restrictions on competition, it seems recommendable to keep markets open by a combined employment of different policy instruments. This may include guidelines and interpreting notes of the antitrust authorities concerning the application of competition law in IT markets, developing comprehensive principles for incorporating requirements regarding interoperability and support of open file formats into the public procurement of IT products, and maybe as well public information policy regarding Trusted Computing inter alia by updating the 2004 statement of the Federal Government on TCG and NGSCB.

Finally, it seems advisable to make all dispositions which are necessary for an immediate opening of competition law procedures in case of an indication of an actual restriction of competition.

3 Hintergrund der Studie

Viele Informations- und Kommunikationsprozesse des öffentlichen, wirtschaftlichen und privaten Lebens sind heute ohne Informations- und Telekommunikationstechnologien nicht mehr denkbar. Rund 1,2 Mrd. Menschen nutzen heute weltweit das Internet für wirtschaftliche und private Zwecke und versenden beispielsweise 130 Mrd. E-Mails pro Tag. Vertraulichkeit, Integrität und Verfügbarkeit bilden daher essentielle Faktoren der Informationsgesellschaft, die zur Aufrechterhaltung moderner Geschäftsprozesse und beim Transport sowie der Speicherung sensibler Daten etwa in Zusammenhang mit E-Government oder E-Commerce unabdingbar geworden sind.

Parallel zur wachsenden Abhängigkeit unserer Gesellschaft von der Verfügbarkeit der Telekommunikationsinfrastruktur nehmen im Zuge der weltweiten Nutzung des Internet die Bedrohungen durch Malware, Spyware, DoS-Angriffe etc. (Viren, Würmer, Trojaner, Phishing) kontinuierlich zu. Rund 30 neue Viren werden pro Tag über das Internet verbreitet, der dadurch entstandene Schaden wird alleine für den Unternehmensbereich für das Jahr 2006 in den USA auf über 67 Mrd. US$ geschätzt. Das Bundeskriminalamt (BKA) stellt in seinem Bundeslagebild Wirtschaftskriminalität (PKS-Auszug) für das Jahr 2006 fest, dass durch Wirtschaftskriminalitätsdelikte in Deutschland im vergangenen Jahr ein Schaden in Höhe von 4,3 Mrd. Euro verursacht wurde.[3] Experten prognostizieren, dass schon mittelfristig ähnliche Entwicklungen im mobilen Internet Platz greifen werden.

Nach dem neuesten Bericht des BSI hat sich insbesondere die Motivationslage der Angreifer verändert und an die Stelle des „sportlichen Ehrgeizes“ einzelner Hacker ist die hoch professionalisierte und organisierte Kriminalität getreten.[4] So wurden 2006 fast 100 Mio. Diebstähle persönlicher Identitäten registriert. Die Bedrohungslage hat sich hierdurch, aber auch durch die steigende Komplexität der Betriebssysteme, durch Sicherheitslücken in Browsern, durch neue Anwendungen sowie durch nomadischen und mobilen Zugang zu konvergenten Netzen kontinuierlich verschärft. Hierdurch ergeben sich deutlich wachsende Anforderungen an die Sicherheit, die Verfügbarkeit und die Vertrauenswürdigkeit der eingesetzten IT-Infrastruktur, der entsprechenden IT-Komponenten sowie der Endgeräte.

Die Schaffung einer vertrauenswürdigen Systemumgebung, der Schutz der Hardwareplattformen und die Herstellung sicherer IT-Komponenten stellt zweifellos eine der größten Herausforderungen für Hersteller und Anwender dar. Es hat sich im Lauf der letzten Jahre gezeigt, dass Sicherungsstrategien, sei es als Software-Zertifizierungsprogramme, sei es als reine Softwarelösungen etwa mittels Firewall, Anti-Viren- oder

---

3 Die mittels Internet in Deutschland begangenen Straftaten werden in der Statistik des Bundeskriminalamtes in der Wirtschaftskriminalität erfasst. Vgl. BKA 2007, S. 3f. Die dort ermittelte Zahl der Fälle verdoppelte sich von 2005 (4.600) bis 2006 (9.700).

4 Vgl. BSI 2007: Die Lage der IT-Sicherheit in Deutschland 2007, Bad Godesberg.

Anti-Spam-Programmen als nicht tiefreichend genug angesehen werden können. Vielmehr muss jede Sicherheitsstrategie „tiefer“ ansetzen und durch die Sicherung der Integrität der physischen IT-Plattformen gegen ihre Kompromittierung die Voraussetzungen für eine vertrauenswürdige Verwendung („Trusted Computing“) schaffen.

Durch die Herstellung eines sicheren physischen Kerns, einer sog. „Root of Trust“ soll – bis zu einem gewissen Sicherheitsniveau - der Ansatzpunkt (Anker) für die Etablierung einer Sicherheitskette („Chain of Trust“) geschaffen werden, der gegenüber heutigen Lösungen einen erheblichen Zugewinn an Sicherheit bedeutet.

Trusted-Computing-Plattformen umfassen hierbei nicht nur stationäre Rechner-, Server- und Hostsysteme, sondern prinzipiell alle rechnerbasierten Systeme und insbesondere auch die Vielzahl mobiler Endgeräte für den Remote Access. Trusted Computing-Plattformen werden durch den Einbau eines separaten Sicherheitsmoduls, d. h., die feste Implementierung eines Smart Card-ähnlichen Moduls in die Rechnerarchitektur geschaffen. Dieses sog. Trusted Platform Module (TPM) ermöglicht sicheres Booten, erzeugt und verwaltet - vereinfacht - kryptografische Schlüssel, Zertifikate und Referenzwerte, signiert Dokumente, verifiziert entsprechende Signaturen und kann bei Bedarf zahlreiche weitere Funktionalitäten (Migrationsfunktionen für Schlüssel, Authentifikation etc.) zur Verfügung stellen. Damit würde eine vertrauenswürdige Plattform zur Verfügung stehen, von der man weiß, dass sie nicht kompromittiert wurde.

Nicht nur können auf diese Weise wichtige Applikationen vor böswilligen Codes abgekapselt werden, es können auch kritische Daten (z. B. biometrische Templates) sicher gespeichert, Ausführungsregeln abgesichert oder Signatur- und Kryptierfunktionalitäten vorgehalten werden. Um den Sicherheitsgewinn der durch TPM veränderten Systemarchitektur auszuschöpfen, sind jedoch weitere Anpassungen auf der Ebene der jeweiligen Betriebssysteme sowie der Anwendungssoftware erforderlich.

Viele Experten sind sich heute einig, dass es zur Entwicklungsstrategie sicherer Plattformen mittels Mikrokernel-Technologie und/oder TPMs keine überzeugenden Alternativen gibt. Verschiedene Argumente sprechen dafür, die erheblichen Sicherheitszugewinne, die TC für private und geschäftliche Anwendungen etwa bei Transaktionsdiensten bietet, so schnell wie möglich auszuschöpfen und dem Markt entsprechende Lösungen zur Verfügung zu stellen. Kritische Argumente hingegen verweisen darauf, dass TC eher dazu dienen soll, die Geschäftsinteressen und (künftigen) Geschäftsmodelle marktmächtiger industrieller Akteure der IT- und Content-Branche in globalem Maßstab durchzusetzen.[5] Allerdings sind diese Stimmen etwa seit dem Jahr 2004 verstummt. Statt weiter über Risiken nachzudenken wird vermehrt über die Chancen von TC und die dafür erforderlichen Einsatz- und Rahmenbedingungen nachgedacht.

---

5 Vgl. z. B. Anderson, R. (2006): Trusted Computing FAQ 1.1 (TC/TCG, TCPA/Palladium/NGSCB/-LaGrande) http://hipjoint.de/tcpa-palladium-faq-de.html.

Der EU und insbesondere Deutschland kommt beim Bestreben eines rationalen Umgangs mit Trusted Computing im internationalen Vergleich eine Vorreiterrolle zu. In den letzten Jahren sind eine Reihe einschlägiger F&E-Projekte angestoßen und finanziert worden. So können das EU-Projekt „Open Trusted Computing“ sowie das von der Bundesregierung geförderte Projekt EMSCB/TURAYA als Beiträge betrachtet werden, die Potenziale einer offenen, für alle Anwender verfügbaren und sichereren IT-Plattform auszuloten.

Diese Initiativen sind insbesondere auch deshalb von Bedeutung, weil einige große Chip- und Hardware-Hersteller bereits heute Fakten für die künftige Marktstruktur schaffen. So wurden 2006 weltweit bereits 100 Mio. TP Module verbaut. Obwohl diese noch nicht (vollständig) in die Betriebssysteme integriert sind, gelten TPMs inzwischen als Massenprodukte, die in vielen IT-Systemen unbemerkt und standardmäßig verbaut werden.[6] Als problematisch müssen daher auch Überlegungen angesehen werden, TPMs in anderen Serienkomponenten wie Chipsätze, die CPU oder I/O-Chips zu integrieren.

Die Bundesregierung war in den letzten Jahren bemüht, die kontroversen und sehr komplexen Diskussionen zu den mit den Standardisierungsaktivitäten der TCG verbundenen datenschutzrechtlichen, verbraucherpolitischen, wettbewerbsrechtlichen sowie industriepolitischen Implikationen aufzuhellen und zu versachlichen.[7]

Im Rahmen mehrerer Symposien und Workshops[8] wurden offen z. B. die Befürchtungen diskutiert, dass das TCG-Konzept Open Source-Produkte vom Markt ausschließt, dass es Nutzern die Verfügungshoheit über ihre Endgeräte entzieht, dass DRM-restringierende Funktionalitäten eine der Hauptzielsetzung marktmächtiger Akteure darstellen oder bestimmte Sicherheitsfunktionen (Remote Attestation) nicht ohne Online-Verbindung genutzt werden können.

Insbesondere wurde deutlich, dass das TCG-Konzept noch keineswegs die „endgültige“ Sicherheits-Plattform beinhaltet, sondern dass die hierzu erforderliche Entwicklung und Implementierung langwierige Prozesse darstellen, die noch vor der Lösung zahlreicher technischer, institutioneller, innovationspolitischer sowie rechtlicher Hürden stehen.[9]

Wichtige Fragen in Hinblick auf die Implikationen künftiger technischer und organisatorischer Entwicklungen sowie unterschiedlicher Anbieterstrategien sind weiter offen und

---

6 Vgl. www.BSI.de/sichere_plattformen/trustcomp/infos. Hierzu auch: TeleTrusT Deutschland (2007): Trusted Computing Whitepaper, Erfurt.

7 Vgl. z. B. das „Eckpunktepapier „Trusted Computing“ der Bundesregierung, 4.9.2004.

8 Vgl. zuletzt: Trusted Computing (TC) Workshop im Rahmen der deutschen EU-Ratspräsidentschaft, Berlin 26. und 27.2.2007.

9 Eine Untersuchung der Universität Bochum im Jahr 2006 zeigt beispielsweise, dass nicht alle der im Markt anzutreffenden TPM vollständig den TCG-Spezifikationen folgen. Daher sind Überlegungen sinnvoll, die korrekte Arbeitsweise von TPMs durch zertifizierte Testsuites einer Prüfung zu unterziehen. Vgl. BfDI (2006): Tätigkeitsbericht 2005-2006, Berlin.

stellen für die Wirtschaftspolitik auch in Zukunft eine große Herausforderung und zahlreiche Unwägbarkeiten dar.[10]

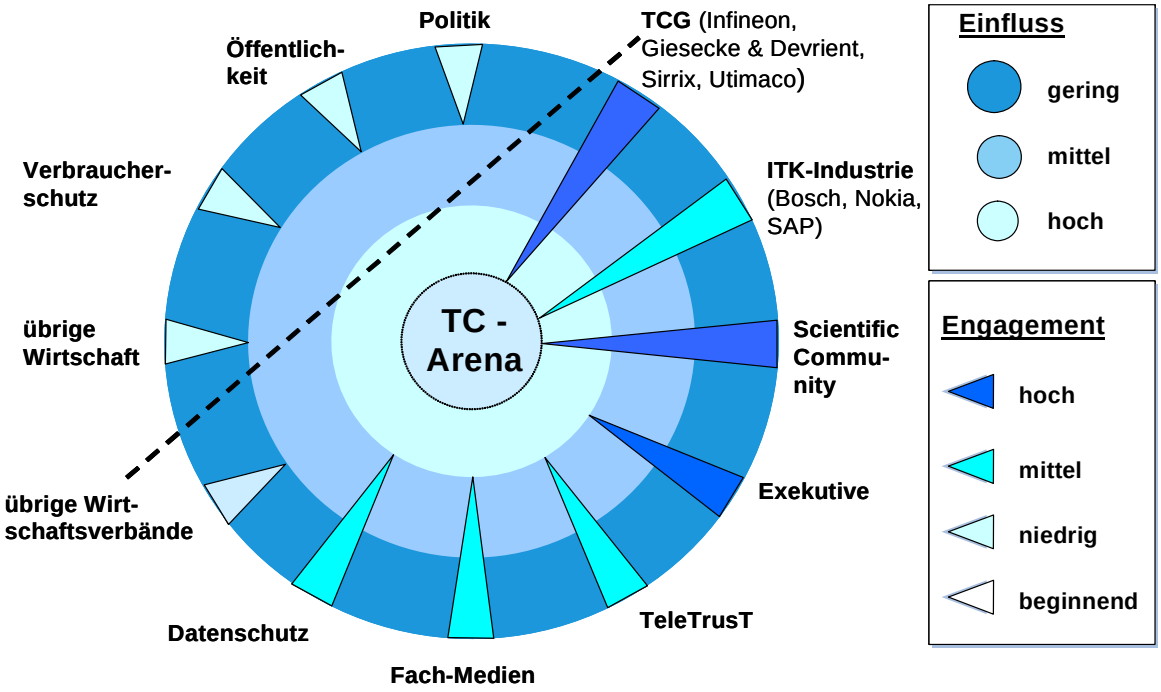
Hierzu gehören folgende Gesichtspunkte:

- Chancen und Risiken für einzelne Wirtschaftsbranchen in Deutschland (wie z. B. IT-Industrie, Smart Card-Industrie, KMU-Software-Hersteller, Open-Source-Software(OSS)-Produkte, Einsatzfelder in anderen Branchen etc.),
- wettbewerbliche und industriepolitische Implikationen von TC sowie die möglichen Folgen einer oligopolistischen Angebotsstruktur,
- organisatorische und institutionelle Strukturen der informationellen Besser- bzw. Gleichstellung für TCG-Nichtmitglieder (höhere Transparenz, Verringerung des Informationsvorsprungs, verbesserter Know how-Transfer),
- Ausgestaltung einer transparenten, nicht-diskriminierenden Lizenzierungspolitik insbesondere auch in Hinblick auf KMU und OSS-Anbieter,
- Modellierung alternativer Standardisierungsstrukturen wie z. B. eines wettbewerbskonformen und innovationsdynamischen Technologiepools,
- TC-relevante, wettbewerbspolitische und –rechtliche Entwicklungen insbesondere im Licht der aktuellen Rechtsprechung zu Kartellverbot und Missbrauch einer marktbeherrschenden Stellung,
- Konformität von TPM mit den Spezifikationen der TCG,
- Realisierungsformen privatwirtschaftlich organisierter Konfliktlösungen zwischen involvierten Marktteilnehmern,
- Verbraucherschutz und Konsumentensouveränität (faktische Relevanz der Wahlfreiheit (Opt-In) bei Dominanz von TPM-basierten Geschäftsmodellen („Befürchtung eines sozialen Kontrollverlusts“)),
- Implikationen des Einsatzes von TPM für den Datenschutz,
- Ziel der vorliegenden Studie ist es, diese Aspekte zu untersuchen, Informationen zu diskutieren, Einschätzungen zu gewinnen und auf die damit verbundenen Fragestellungen (Teil-)Antworten zu finden. Hierzu wurden alle verfügbaren relevanten Informationsquellen genutzt. Auf Grund der hohen Komplexität vieler Aspekte sowie der vielfach auch unklaren Datenlage wurden mit den unterschiedlichen Stakeholdern (unterhalb der gestrichelten Linie; vgl. Abbildung 3-1) zahlreiche strukturierte Experteninterviews durchgeführt. Hierfür sei den Mitwirkenden für ihre Zeit und Engagement gedankt.

---

10 Vgl. Sandl, U.: Die Trusted Computing Group (TCG). Eine Herausforderung auch für die deutsche Wirtschaftspolitik, in, DuD, 28 (2004) 9, S. 521-524.

Abbildung 3-1: Struktur und Akteure der deutschen TC-Arena



Quelle: WIK-Consult

Die Studie wurde von Juli 2007 bis März 2008 durchgeführt. Sie basiert zum einen auf einer systematischen Auswertung und Analyse der öffentlich verfügbaren Sekundärquellen sowie der Online-Recherche. Zum zweiten wurden im Rahmen der Studie mehr als zwei Dutzend Expertengespräche mit wichtigen TC-Akteuren auf der Basis eines strukturierten Leitfadens durchgeführt. Diese Akteure stammen aus der Wissenschaft, der Wirtschaft sowie der Verwaltung und wurden vorab mit dem Auftraggeber ausgewählt. Der rechtswissenschaftliche Teil (Kap. 8) wurde hierbei durch IRNIK erstellt.

Die (Zwischen-)Ergebnisse wurden auf einem internen Workshop des BMWi in Bonn sowie einer Arbeitsgruppenveranstaltung des BITKOM zur IT-Sicherheit in Frankfurt vorgestellt und diskutiert.

4 Die Genese von Trusted Computing und die Trusted Computing Group

Die Anfänge der Idee, für eine vertrauenswürdige Informations- und Datenverarbeitung (Trusted Computing) entsprechende technische Plattformen zu schaffen, reichen bis weit in die achtziger Jahre zurück. Aber erst mit der Realisierung weltumspannender Kommunikationsnetze und dem seither beobachtbaren Wettlauf zwischen den Bemühungen zum Schutz vor Kompromittierung auf der einen und den immer ausgeklügelteren Angriffsmethoden auf der anderen Seite, hat der Druck für konkrete und nachhaltige Maßnahmen zur Generierung und zum Schutz von Vertrauen in Infrastrukturen und Kommunikationsgeräte entscheidend zugenommen. Es geht darum, einen Zustand zu erreichen, dass „einer Plattform vertraut werden kann, wenn sie sich bezogen auf einen bestimmten Zweck immer in der gleichen Weise verhält“.[11]

Vor diesem Hintergrund riefen 1999 die fünf führenden amerikanischen IT-Konzerne Compaq Computer Corporation, Hewlett-Packard (HP), IBM Corporation, Intel Corporation und die Microsoft Corporation die sog. Trusted Computing Platform Alliance (TCPA) ins Leben. Ziel der TCPA war die Herstellung vertrauenswürdiger Komponenten für alle Computer- und Kommunikationssysteme.

Die Organisationsstruktur der TCPA stellte sich jedoch auf Grund des „Einstimmigkeitsprinzips“ als zu unbeweglich und wegen ihrer Größe als zu ineffizient heraus, so dass ihre Standardisierungsaktivitäten – nicht zuletzt durch ihre wenig transparente und auf die Durchsetzung ihrer eigenen Geschäftsmodelle hin bedachte Arbeit – in die Kritik durch die Fachwelt geriet.

Im Jahr 2003 wurde die TCPA daher durch die Gründung der neuen Trusted Computing Group (TCG[12]) ersetzt, die auf Grund des Mehrheitsprinzips (2/3-Mehrheitsbeschlüsse) bei Abstimmungsprozessen zugleich als handlungsfähiger galt.[13] Die TCG hat in der Folge alle Standardisierungs- und Spezifizierungsaufgaben der TCPA übernommen. Dabei stand die folgende Zielsetzung im Vordergrund: „Die Mitglieder der Trusted Computing Group entwickeln und treiben die Verbreitung eines offenen, Hersteller-neutralen Industriestandards für die Gestaltung der technischen Grundeinheiten und der Programmierschnittstellen für unterschiedliche Plattformen voran“.[14]

Die Arbeiten der TCG fokussieren demnach auf Hardware-Komponenten, die nach den Common Criteria (bis CC EAL4+) evaluiert werden sollen, damit Funktionen und Implementierung jederzeit nachvollziehbar sind.

---

11 Vgl. Rosteck 2007, S. 13 (Übersetzung aus dem Englischen durch die Autoren).
12 Vgl. https://www.trustedcomputinggroup.org.
13 Vgl. Rosteck, 2007.
14 Vgl. https://www.trustedcomputinggroup.org/home (Übersetzung aus dem Englischen durch die Autoren).

Die TCG wird von einem Board of Directors (BOD) gesteuert, welche wiederum von einem Technical Committee unterstützt werden. Die genuinen Standardisierungsvorgänge und Spezifikationen finden in Arbeitsgruppen statt. Derzeit existieren neun Arbeitsgruppen, die die Standardisierungsbemühungen für die Hardware-Plattformen Fotokopierer, PC Clients, Speichermedien, Infrastruktur, Server, vertrauenswürdige Kommunikationsnetze, mobile Endgeräte, Software Stacks sowie Trusted Platform Modules vorantreiben (vgl. Tabelle 3.1).[15]

Tabelle 4-1: Die Trusted Computing Plattform nach Arbeitsgruppen

Plattform	**Kurzbeschreibung der Aktivitäten und Spezifikationen**
Hard Copy	Offene, herstellerunabhängige Spezifikationen für Kopiergeräte
Infrastructure	Architekturmodelle, Schnittstellen und Metadaten, um Infrastrukturbrüche zu überbrücken
Mobile	Anpassung des TCG-Konzepts an mobile Endgeräte und deren Besonderheiten
PC Client	Allgemeine Funktionalitäten, Schnittstellen und die Mindestsicherheits- und Datenschutzanforderungen für PCs mit TCG-Komponenten
Server	Definitionen, Spezifikationen, Richtlinien und technische Anleitungen zur Implementierung von TGC-Technologie in Servern
Software Stack	Bereitstellung von Standard-Programmierschnittstellen für Hersteller von Anwendungen, die ein TPM nutzen möchten. Ziel ist die Entwicklung einer herstellerneutralen Spezifikation, die es ermöglicht, TC-Anwendungen zu entwickeln, die auf jeder Hardware und mit jedem Betriebssystem laufen.
Storage	Entwicklung von Standards und Verfahren, um die gleichen Sicherheitsdienste auf unterschiedlichen Datenträgern gewährleisten zu können
Trusted Network Connect	Definition und Veröffentlichung einer offenen Architektur und einer wachsenden Zahl an Standards für Ende-zu-Ende-Integrität sowie die herstellerunabhängige Interoperabilität für eine breite Auswahl an Endpunkten, Netztechnologien und Verfahren.
Trusted Platform Module (TPM)	Definition der TPM Architektur

Quelle: TCG

Eine der wichtigsten organisatorischen Veränderungen gegenüber der TCPA besteht in der Öffnung der Standardisierungsarbeit der TCG für alle Akteure der internationalen ITK-Branche:

15 Zur inhaltlichen Beschreibung der Arbeitsgruppen vgl. Work Group Charter Summary, https://www.trustedcomputinggroup.org/home.

- Auf der obersten Ebene agieren die „Promotoren“, die nur auf Einladung durch den Board mitwirken und dort sowie im Technical Committee einen Sitz erhalten. Der Lenkungsgruppe der „Promoter“ gehört der deutsche Chip-Hersteller Infineon an, der seit November 2005 auch ein Mitglied in den Board of Directors entsendet. Den Promotoren gehören ferner die Unternehmen AMD, Hewlett-Packard, IBM, Intel Corporation, Lenovo Holdings Ltd., Microsoft sowie Sun Microsystems Inc. an.

- Neben den Promotoren arbeiten die „Contributoren“ aktiv in den Arbeitsgruppen mit und haben Einblick in den jeweils aktuellen Stand der Spezifikationen. Der Gruppe der mitgestaltenden Unternehmen gehören die deutschen Firmen Fujitsu Siemens Computers, Giesecke & Devrient sowie Utimaco Safeware, aber auch z. B. große europäische Unternehmen wie France Telecom, Ericsson oder Nokia an.[16]

- Als dritte Gruppe sind die Adaptoren zu nennen, die durch ihre Mitgliedschaft in der TCG frühzeitig Kenntnis von neuen Spezifikationen erhalten. Deutsche Unternehmen sind hier z. B. AUCONET oder die Sirrix AG (vgl. Tabelle 4-2).

Tabelle 4-2: Mitglieder der TCG nach Herkunftsländern und Status

Land	Promoter	Kontributoren	Adopter
USA	7	48	34
China	1	1	0
Deutschland	1	4	3
Japan	0	10	1
UK	0	4	3
Taiwan	0	3	1
Finnland	0	2	0
Kanada	0	2	4
Korea	0	2	1
Niederlande	0	2	1
Schweiz	0	2	0
Frankreich	0	1	1
Schweden	0	1	0
Norwegen	0	0	2
Israel	0	0	1

Quelle: TCG (Stand 11/2007)

16 Vgl. www.trustedcomputinggroup.org.

Insgesamt arbeiten nach Angaben der TCG heute rund 170 ITK-Unternehmen in der TCG mit, davon mehr als die Hälfte aus den USA. Elf Akteure kommen aus Japan, acht aus Deutschland sowie sieben aus UK. Der Mitgliedsbeitrag orientiert sich abgestuft am Level der Mitgliedschaft. Damit kleine und mittelständische Unternehmen mit weniger als 100 Angestellten nicht durch zu hohe Gebühren von ihrer Mitwirkung abgehalten werden, können diese gegen eine Jahresgebühr von lediglich 1000 US$ in der Gruppe der Adoptoren mitwirken.

Um die Kommunikations- und Diskussionsbasis zu verbreitern und um auch Regierungsorganisationen sowie Hochschulen einzubeziehen, wurde das sog. Liaison-Programm ins Leben gerufen. Diesen Institutionen ist es erlaubt, aktiv in den Arbeitsgruppen mitzuwirken. Eine Unterstützung von Hochschulen bzw. Forschung und Lehre findet im Rahmen des sog. Mentor-Programms statt, bei der TCG-Mitgliedsfirmen entsprechende Beratungsfunktionen erbringen.

Schließlich wurde ein Advisory Board („Enderle Group“) eingerichtet, in dem namhafte Experten der ITK-Branche mit i. d. R. internationalem Hintergrund vertreten sind, die die TCG beraten. Von deutscher Seite wirkt dort ein Vertreter von W3C mit.

Eine besondere Bedeutung für TC besitzt die Spezifikation eines sicheren Hardware-Chips, dem sog. Trusted Platform Module (TPM). Die Standardisierungsarbeiten der TCG sind im Bereich des TPMs vergleichsweise weit vorangeschritten. 2002 bzw. 2003 wurden die Standards 1.1b sowie 1.2 (2003) veröffentlicht, deren umfängliche Dokumentationen allerdings große Anforderungen an die interessierten Akteure stellen. Das Trusted Platform Module übernimmt im wesentlichen fünf Funktionen:

- die Überprüfung und das sichere Speichern einer als vertrauenswürdig eingestuften Systemkonfiguration,
- die Bereitstellung eines Hardware-geschützten Speicherbereichs,
- den Schutz und die Generierung von symmetrischen und asymmetrischen Schlüsseln,
- die Bereitstellung eines speziellen Schlüssels, mit dem Dritte eine Plattform als vertrauenswürdig erkennen können, sowie
- Verwaltungsfunktionen, mit denen sich z. B. das TPM vom Nutzer ein- und ausschalten lässt.[17]

17 Vgl. www.bsi.de/sichere_plattformen/trustcomp/info/tcgi.htm.

TPM-Chips sind heute standardmäßig in neu beschafften IT-Systemen wie z. B. Notebooks integriert. Mittelfristig, d. h. bis spätestens 2015, kann auf Grund der vergleichsweise kurzen Lebenszyklen der IT-Hardware von einer flächendeckenden Verfügbarkeit ausgegangen werden.

Insgesamt gelten die Arbeiten der TCG als zentral für den Fortschritt und für Innovationen im Bereich TC. Nur wenn alle Teile der heute immer komplexeren und immer stärker vernetzten IT-Landschaft sich ergänzen, sich gegenseitig stützen und gut durchdacht zusammenwirken, ist es möglich, Netzarchitekturen und Computersysteme zu entwickeln, die trotz einer ständigen Bedrohung durch Dritte bzw. durch fehlerhafte Applikationen ihre Funktionen korrekt aufrechterhalten.

Die durch die TCG-Standards ermöglichten Mechanismen schaffen die Voraussetzungen, „um unter ingenieursmäßigen Randbedingungen vertrauenswürdige Systeme zielorientiert entwickeln zu können und damit auch bei der Konstruktion von Datenverarbeitungssystemen Vertrauen und korrekte Funktionalität nicht nur „hineinzutesten“, sondern mit systematischen Methoden und einem beschränkten Ressourcen-Aufwand sichere Systeme gezielt zu entwickeln.“[18]

18 Vgl. Brandl 2007, S. 39.

5 Trusted Computing in Deutschland

5.1 Trusted Computing in der Perspektive der Forschung

Im Bereich der Forschung konzentrieren sich die Aktivitäten zu Trusted Computing im Kern auf vier Institutionen: Zum einen auf die Aktivitäten am Lehrstuhl für Betriebssysteme an der Technische Universität Dresden, am Horst Görtz Institut für Sicherheit in der Informationstechnik an der Ruhruniversität Bochum, am Institut für Internet-Sicherheit an der Fachhochschule Gelsenkirchen sowie am Fraunhofer-Institut für Sichere Informationstechnologie SIT in Darmstadt.

5.1.1 Schwerpunkte und Arbeiten an der Technischen Universität Dresden

5.1.1.1 Institutionelle Verankerung

Die Technische Universität Dresden (TUD) besitzt in der 1990 gegründeten Fakultät für Informatik mit insgesamt 3.100 Studierenden über einen der größten Fachschwerpunkte für Informatikausbildung in Deutschland. In den sechs Instituten der Fakultät sind insgesamt 28 Professoren und Dozenten sowie über 260 Mitarbeiter beschäftigt. Das Institut für Systemarchitektur ist diejenige Einrichtung an der TUD, die sich mit Fragen der IT-Systemsicherheit befasst. Insgesamt stehen dort fünf Lehrstühle bzw. Professuren zur Verfügung, die sich mit den Bereichen

- Betriebssysteme,
- Datenbanken,
- Datenschutz und Datensicherheit,
- Rechnernetze, sowie
- System Engineering befassen.

Die einschlägigen Aktivitäten zu TC sind am Lehrstuhl für Betriebssysteme angesiedelt, deren Inhaber derzeit Prof. Dr. Hermann Härtig ist. Mit der Thematik „Sichere Systeme“ sind an der TUD aktuell insgesamt etwa 20 Personen befasst.[19]

---

19 Vgl. http://www.inf.tu-dresden.de/index.php?node_id=1141.

5.1.1.2 Schwerpunkte der Aktivitäten

Die besonderen Forschungsschwerpunkte am Lehrstuhl für Betriebssysteme bestehen aktuell in der Erforschung bzw. Entwicklung von

- Echtzeitsystemen,
- Sicherheit in Betriebssystemen, sowie
- Mikrokern-basierten Betriebssystemen.

Im Mittelpunkt der theoretischen Befassung (mathematischen Modellierung) mit verteilten Betriebssystemen sowie Echtzeitsystemen stehen Fragen der Skalierbarkeit verteilter Systeme, Fehlertoleranzverfahren, Parallelrechnerbetriebssysteme sowie die Sicherheit in verteilten Betriebssystemen. Bei den eher Entwicklungs-orientierten Aktivitäten geht es insbesondere um Aspekte der Konstruktion und Implementierung sog. Mikrokern-basierter Betriebssysteme, denen für die Realisierung, Umsetzung und Anwendung von TC eine zentrale Bedeutung zukommt.

Eine Grundidee des F&E-Ansatzes Mikrokern-basierter Betriebssysteme besteht – vereinfacht – darin, dass die heute im Markt verfügbaren Betriebssysteme wie z. B. Windows XP oder Linux über eine so große Anzahl von Programmzeilen verfügen, dass deren Überschaubarkeit und Transparenz im Sinne einer Verifikation von Verfügbarkeit und von Sicherheit kaum mehr darstellbar ist.[20]

Grundlage der neuen Technologie ist daher die Idee, große monolithische Betriebssysteme in kleinere Komponenten zu zerlegen, um so durch Transparenz eine höhere Verlässlichkeit der Systeme zu erreichen. Gemeinsame Grundlage dieser Komponenten ist ein “Mikrokern”, der für die Isolierung der Komponenten untereinander sorgt und als einzige Komponente über alle Hardware-Privilegien verfügt.

Dementsprechend werden in einem Mikrokern-basierten Betriebssystem verschiedene Funktionalitäten aus den bestehenden monolithischen Betriebssystemkonzepten herausgelöst („Separation“) und stark verkleinert neu programmiert („Downsizing“). Ein solcher Mikrokern umfasst kaum mehr als 20.000 Zeilen Quelltext und stellt nur Funktionen zur Prozessverwaltung und bestimmte Funktionen für die Synchronisation und die Kommunikation bereit. Alle weiteren Systembestandteile wie z. B. die Speicherverwaltung, Programm-Loader, Geräteverwaltung sowie Anwendungen laufen nach dem Bootvorgang nicht als privilegierte Kernmodule, sondern in abgeschotteten User-Level-Speicherbereichen.

---

20 So verfügt z. B. ein aktueller Linux-Kernel über mehrere Millionen Programmzeilen, während Microsoft-Produkte diese noch um mehrere Faktoren übersteigen.

Auf diese Weise wird es möglich, die steuer- und sicherheitsrelevanten Bestandteile eines herkömmlichen Betriebssystems (Linux, Microsoft) zu isolieren, zu verkleinern und als eigenes Betriebssystem für einen formalen Reviewprozess zugänglich zu machen, der sonst auf Grund der enormen Ressourcen- und Kapazitätsanforderungen wenig Aussicht auf Erfolg hätte.

Eine Anwendung von besonderer Bedeutung, aber sicherlich nicht die einzige, ist Virtualisierung, eine Technik, die die Wiederverwendung vorhandener Software (Betriebssysteme und ihre Anwendungen) ohne oder mit nur geringen Anpassungen ermöglicht. Dies ist deshalb von Bedeutung, weil z. B. die Abwärtskompatibilität von neuen Betriebssystemen Sicherheitsprobleme mit sich bringt.

Mikrokernbasierte Technik erlaubt es, sicherheitskritische oder echtzeitfähige Anwendungen neben herkömmlicher Software zu nutzen. Die für die neuen Anwendungen kritischen Komponenten (Trusted Computing Base) kann viel kleiner gehalten werden als mit herkömmlicher Software mit der Hoffnung, dass die potenzielle Gefährdung durch Fehler und Angriffe ebenfalls deutlich kleiner gehalten werden kann.

Eine weit verbreitete Ausprägung dieser Technologie basiert auf dem Mikrokern “L4” und “L4Linux”, einer Variante des Betriebssystem Linux. Diese ist so modifiziert, dass sie auf L4 ausführbar wird und damit vorhandene Linux-Anwendungen unterstützt. Die Grundlagenforschung für diese Technologie wurde von den Universitäten in Dresden, Karlsruhe und Sydney sowie an der damaligen GMD und einem IBM-Labor in New York durchgeführt. Im Rahmen des DFG Sonderforschungsbereichs SFB 358 an der TU Dresden wurden die erste Hochsprachenimplementierung für die L4-Schnittstelle “L4/Fiasco”[21] und die erste Portierung des Betriebssystems L4Linux entwickelt, womit die Lizenzunabhängigkeit von der GMD und insbesondere von IBM erreicht wurde. In der Fachwelt genießt diese Entwicklung seither große Anerkennung.

Im März 2006 wurde der Öffentlichkeit erstmals eine Demonstrationsversion des sicherheitsoptimierten Betriebssystems TUD:OS vorgestellt, die seither für Anschauungszwecke zum Download auf dem Portal der TUD zur Verfügung steht. Heute wird die Dresdner Software unter Gnu Public License (GPL, V2) verteilt.

Die Verkleinerung von Betriebssystemen bedeutet einen großen Sprung beim Sicherheitszugewinn, da zwischen die Hardware und die herkömmlichen Betriebssysteme ein Mikrokern geschoben wird, der ausschließlich über die entsprechenden Hardware-Privilegien für den Zugriff auf und die Steuerung einer Plattform verfügt. Im Prinzip kommt dieser Prozess einem Virtualisierungsvorgang gleich, da zwar das aufgespielte herkömmliche Betriebssystem die ihm zugedachten Funktionen erfüllt, aber über keinerlei Zugriffsrechte mehr auf die Hardware des entsprechenden Rechners verfügt.

---

21 Vgl. Verified FIASCO, http://os.inf.tu-dresden.de/vfiasco.

Die Entwickler an der TUD gehen davon aus, dass ein solcher Ansatz die erforderliche Vertrauenskette verkürzt, die Basisvoraussetzungen für TC auf ein Minimum reduziert und daher auch weit weniger verwundbar ist durch Angriffe auf ein TPM bzw. ein BIOS. Zu diesem Zweck wurde ein Bootloader, der sog. Open Secure LOader (OSLO) entwickelt, der ebenfalls öffentlich verfügbar ist.[22]

5.1.1.3 Vernetzung mit anderen Akteuren

Während die Vernetzung mit anderen TC-Akteuren in Deutschland auf Grund der vergleichsweise geringen Zahl der TC-Community als gegeben und teilweise auch als kompetitiv beschrieben wird, sind die grenzüberschreitenden Austausch- und Kooperationsaktivitäten an der TUD sehr ausgeprägt. In den Gesprächen wurde deutlich, dass die Aktivitäten zum fachlichen Austausch und zur Vernetzung sowohl mit Universitäten im Ausland (USA[23], Australien[24]) als auch mit Unternehmen im In- und Ausland (Microsoft, Hewlett & Packard, AMD-OSRC (Operating System Research Center)) Teil des normalen Arbeitsalltags sind und auch die TC-Entwicklung berühren.

Besonderes intensive Kooperationsbeziehungen bestehen im Rahmen der europäischen SOKRATES / ERASMUS-Vereinbarungen mit über neun französischen Hochschulen. Zu diesen Hochschulen gehören z. B. EISTI (École Internationale des Sciences du Traitement de l'Information), ENST (École National Supérieur des Télécommunications), ESIEE (École d'Ingénieurs des Sciences et Technologies de l'Information et de la Communication) oder das Institut National des Sciences Appliquées de Rennes (INSA).

Auch ist ein gewisse personelle Fluktuation des akademischen Nachwuchses von der Hochschule zu Unternehmen wie AMD-OSRC erkennbar. Umgekehrt suchen Unternehmen wie AMD-OSRC aktiv den Kontakt zur Hochschule und stellen beispielsweise auch Hardware-Prototypen für Versuchs- und Entwicklungsaktivitäten an der TUD zur Verfügung. Insofern erweist sich die Nähe zum IT-Standort Dresden mit der Niederlassung des Chip-Herstellers AMD, aber auch zahlreicher anderer Industrieunternehmen (s. u.) als ein wichtiger Vorteil für die F&E-Aktivitäten des Lehrstuhls.

Wichtige Auftrag- bzw. Mittelgeber sowie Projektpartner des Lehrstuhls in der Vergangenheit waren bzw. sind u. a.

- Bundesministerium für Wirtschaft und Technologie,
- Bundesamt für Sicherheit in der Informationstechnik,

---

22 Vgl. Kauer, 2006, http://os.inf.tu-dresden.de/~kauer/oslo.
23 Z. B. die University of California, die Arizona State University und die University of Texas.
24 Z. B. die University of New South Wales (UNSW), die Macquarie University Canberra, die Deakin University sowie University of Queensland.

- Deutsche Forschungsgemeinschaft,
- EU (Open Trusted Computing)(OTC)),
- SAP AG,
- IBM Corporation Germany und IBM Corporation USA ,
- Deutsche Telekom und T-Systems,
- AMD Saxony Manufacturing GmbH,
- Infineon Technologies Dresden GmbH & Co. OHG,
- intel Corporation USA,
- HP Corporation USA,
- Siemens AG,
- sd&m AG,
- net-Linux,
- Daimler Chrysler AG ,
- secunet Security Networks AG.

Die auf L4 basierende Mikrokern-Technologie weckte in den letzten Jahren erhebliches Interesse deutscher und internationaler Industrieunternehmen. Auch aufgrund der daraus resultierenden Zusammenarbeit und der damit verbundenen Nutzung in industriellen Forschungsprojekten gewannen L4 und Co in Bezug auf Reifegrad und Funktionsumfang. Substantielle europäische und deutsche Forschungsförderung trugen erheblich zu dieser Entwicklung bei. Von einer Produktreife im industriellen Sinn kann allerdings noch nicht gesprochen werden.

Während an der TU Dresden kontinuierlich an der Basisplattform und an prototypischen Demonstratoren weitergearbeitet wurde, wurde von den externen Partnern Anwendungsbereiche und Ergänzungen untersucht und implementiert. Die auf der Dresdner Plattform (Fiasco + L4Env) basierenden Architekturen wurden bisher erfolgreich im Bereich der Echtzeitsysteme (DROPS, Dresden Real-Time Operating Systems) und Sicherheitsarchitekturen (L4/Nizza) eingesetzt. Zur Plattform gehören unter anderem

- der Mikrokern L4/Fiasco,
- eine auf L4 lauffähige Version des Betriebssystems Linux,
- Basisserver (z. B. Speicherverwaltung, Namensdienst etc.),

- eine sichere Benutzeroberfläche (Nitpicker),
- eine Ausführungsumgebung für Linux-Gerätetreiber (DDELinux) und eine darauf aufbauende virtualisierte Geräte-Infrastruktur (Netzwerk, Festplatte, Eingabegeräte).

5.1.1.4 Beispiele für Kooperationsprojekte

µ-SINA: mit secunet und gefördert durch BMWi (Vernet)

In diesem Projekt wurde eine Variante des von der Firma secunet kommerziell vertriebenen Produktes SINA auf die Mikrokerntechnik überführt. Ergebnis war eine VPN-Box mit extrem kleiner Trusted Computing Base.

5.1.1.4.1 L4VM: mit BSI und Innotek/secunet

Dieses Projekt hatte zum Ziel, ein kommerziell verfügbares Virtualisierungspaket mit der Mikrokerntechnologie zu verbinden. Ergebnis war eine proprietäre Implementierung eines Virtual Machine Monitors namens L4VM. Mit Hilfe dieses VMM ist es möglich, binäre Varianten von Windows, Linux und OS/2 auf L4-basierten Systemen auszuführen.

5.1.1.4.2 L4Mobile: mit Infineon und Nokia

Ziel dieser direkt industriell finanzierten Kooperationen mit Herstellern von Mobiltelefonen bzw. Plattformen für Mobiltelefone war die Frage, ob mikrokernbasierte Technologie für diesen Einsatzbereich für die Lösung der dort drängenden Probleme in Frage kommt. Ergebnisse unterliegen teilweise noch Vertraulichkeitsrestriktionen. Die Arbeiten wurden teilweise von einer externen Firma (GWT-TUD) durchgeführt, die den Technologietransfer für die TU Dresden betreibt.

5.1.1.4.3 EMSCB[25] und “TURAYA”[26]

Wesentliches Ziel von EMSCB ist die Verbindung der Mikrokern-Technologie mit Trusted Computing, also Techniken des authentifizierten Urladens, der “Remote Attestation” und des “Sealed Memory”. Das Ergebnis waren Demonstratoren (VPN, Harddisk-Verschlüsselung, Digital Rights Management) und eine wesentliche Härtung der Plattform. Die Ergebnisse des Projektes wurden im deutschen Sprachraum aufwändig

---

25 Vgl. http://www.emscb.de/content/pages/Einleitung.htm Zum Projekt emscb vgl. auch Pohlmann Okt. 2005.
26 Vgl. http://www.emscb.de/content/pages/About-TURAYA-de.htm. Zu TURAYA vgl. z. B. Pohlmann / Linnemann 2007.

unter dem Namen “TURAYA” vermarktet. Parallel wird sie nach Auskunft der TUD durch die Universität international unter “L4/Nizza” publiziert.

Open TC (ca. 25 internationale Partner, gefördert durch die EU[27])

Das EU-Projekt Open TC hat die Verbindung von Techniken des Trusted Computing mit Virtualisierung zum Ziel. Ergebnis wird eine auf zwei Plattformen (L4 und Xen) basierende Architektur sein. Ein weiteres, auf enger Zusammenarbeit mit der örtlichen Entwicklungsabteilung von AMD basierendes Ergebnis war “OSLO” (Open Secure LOader), die erste öffentlich zugängliche Basissoftware für die nächste Hardware-Generation der Trusted Computing Technik (s. o.).

ROBIN (TU Dresden, secunet, ST-Microelectronics, Universität Nijmegen, gefördert durch die EU)[28]

Dieses von der Europäischen Kommission seit 2005 geförderte Verbundprojekt hat zum Ziel, die nunmehr vorliegende, über zehnjährige Erfahrung mit L4, DROPS und L4/Nizza für eine völlige Neuentwicklung zu nutzen. Vorwiegende Ziele sind bei ROBIN (Open Robust Infrastructures), eine Variante der L4/Nizza-Architektur zu implementieren, welche die Möglichkeiten neuer HW-Architekturen, z. B. Support für vollständige Virtualisierung, nutzt. Weiterhin soll eine im Vergleich mit L4VM wesentlich kleinere Trusted Computing Base für Virtualisierung ermöglicht werden. Mit Methoden der theoretischen Informatik sollen Schnittstellen formal spezifiziert und deren Umsetzung im Betriebssystem verifiziert werden. Die Partner secunet und ST-Microelectronics stellen erste Demonstratoren zur Verfügung, welche sie später in Produkte umsetzen wollen.

5.1.1.5 Projektvorschläge zu Forschung, Entwicklung und Einsatzmöglichkeiten mikrokernbasierter Sicherheitsarchitekturen[29]

Die (teilweise) Aufzählung der Kooperationen zeigt das erhebliche Interesse an mikrokernbasierter Technologie. Forschungsbedarf und Einsatzmöglichkeiten im Mikrokern-Bereich gehen weit über das Thema “Trusted Computing” hinaus. Aus der Sicht der TU Dresden gibt es für diese Forschung zwei wichtige Motivationen: Zum einem verschafft sie deutschen Behörden und der deutschen Industrie eigenes, national verfügbares Know-how in Bereich Hochsicherheitssoftwaretechnik, auf die (in einem Notfallszenario) zurückgegriffen werden kann. Zum anderen muss sie mittel- und langfristig auf einen industriellen Einsatz und Export der L4-basierten Technologie abzielen. Zielrichtung ist also,

---

27 Vgl. http://www.Open TC.net/.
28 Vgl. http://robin.tudos.org/.
29 An diesen Projektideen haben die Firmen secunet, Nokia, Infineon, AMD und Ruhr-Universität Bochum (Prof. Bilgic) mitgewirkt und starkes Interesse an einer Teilnahme an neu zu entwickelnden Forschungsprojekten geäußert.

- insbesondere deutschen Unternehmen Zugang zu dieser Technik zu verschaffen,
- technologische Dienstleistungen, also Arbeiten zur Anpassung und Anwendung, zu exportieren,
- deutschen Behörden und deutschen Industrieunternehmen die Option zu geben, kurzfristig auf eine eigene Technologie zurückgreifen zu können, um im internationalen Vergleich wettbewerbsfähig zu bleiben.

Wer spezielle Systeme mit hohen Anforderungen in puncto Sicherheit und Echtzeit benötigt, soll sich die notwendigen Entwicklungen aus Deutschland holen können. Sehr aufwändige Entwicklungen im Ausland (z. B. das französiche “Synapse” Projekt oder die amerikanische MILS Entwicklung) lassen deutliche Anstrengungen erkennen, diese Technik zu erschließen und haben exakt die gleichen Motivationen. Vor diesem Hintergrund bestehen mehrere Themenbereiche mit folgendem Handlungsbedarf:

5.1.1.5.1 Plattformforschung

Die L4-Basistechnologien (Mikrokern und Betriebssystem-Komponenten) sollen auch zukünftig stetig weiter entwickelt und verbessert werden. Die in Dresden vorhandenen Erfahrungen in den Bereichen Sicherheit und Echtzeit sollten weiter konzentriert und vorangetrieben werden.

Eine der Herausforderungen hierbei ist die Unterstützung von vollständiger Virtualisierung durch einen Mikrokern. Weiterhin sollte es zukünftig möglich sein, die Trusted Computing Base (TCB) eines Systems durch die gezielte Verwendung nur bestimmter Komponenten möglichst klein zu halten. Für diese Arbeiten bietet sich die TUDOS Forschungsgruppe an der TU Dresden sowie die Technologietransferfirma GWT-TUD an.

5.1.1.5.2 Einsatz im Behörden- und Enterprisemarkt

Der Einsatz bei Behörden (Auswärtiges Amt, Bundeswehr) kann Schlüsselimpulse für Forschungsprojekte liefern. Gerade im behördlichen und militärischen Umfeld sind Hochsicherheitssysteme - teilweise durch gesetzliche Regularien - gefordert und befinden sich damit partiell auch in einer anderen Wettbewerbssituation. Damit lassen sich im frühen Stadium auch in kleineren Stückzahlen Erfahrungen sammeln und am (kommerziellen) Markt zunächst nicht nachgefragte Sicherheitseigenschaften verkaufen. In diesem Markt steht der Evaluierungs- und Zertifizierungsaspekt im Vordergrund. Hier hat die Firma secunet umfangreiche Erfahrungen mit der Entwicklung und Zulassung dieser Plattformen gesammelt.

5.1.1.5.3 Eingebettete (mobile) Systeme

Die Mikrokern-Technologie ist in der Lage, auch mit sehr beschränkten Ressourcen umgehen zu können und eignet sich deshalb hervorragend für den Einsatz im Bereich der sog. eingebetteten und mobilen Systeme, wo diese Beschränkungen systembedingt sind. Weiterhin bestehen in diesen Gebieten Anforderungen sowohl im Echtzeit- als auch im Sicherheitsbereich: Ein Handy hat beispielsweise nicht nur Echtzeitanforderungen bei der darauf laufenden Software (GSM Stack, Multimedia-Anwendungen), sondern auch Sicherheitsanforderungen vielfältiger Art (Schutz proprietärer Software, Schutz vor Angriffen).

Eine jüngst publizierte Studie von Roland Berger erwartet einen mit 9% jährlich wachsenden Weltmarkt von 135 Mrd. Euro. Die deutsche Industrie wird als sehr gut positioniert eingeschätzt.[30] Sie empfiehlt daher Forschungsförderung in diesem Bereich. Mit der Beherrschung einer Technologie wie der mikrokernbasierten Konstruktion von Systemen insbesondere der TUD-Ausprägung mit Konzentration auf Echtzeitfähigkeit und Sicherheit bietet sich ein hohes Potential an exportierbaren technologischen Dienstleitungen und an direkter Unterstützung deutscher Unternehmen.

Mit Infineon und dem Nokia-Forschungslabor in Bochum gibt es in Deutschland mehrere potente Firmen, die an einer Weiterentwicklung der Technik interessiert sind. Bei den Hochschulen hat sich insbesondere die Fakultät für Elektrotechnik und Informationstechnik an der Ruhr-Universität Bochum unter Leitung von Prof. Dr.-Ing. A. Bilgic bereit erklärt, an den oben beschriebenen Aufgabenstellungen mit zu wirken.

5.1.1.5.4 Hochsicherheitssysteme

Systeme mit höchsten Sicherheitsanforderungen stellen eine weitere Plattform für die Mikrokern-Technologie dar. In Deutschland vorhandenes Know-how aus Verifikationsprojekten wie Isabelle (TU München, Uni Cambridge) und Verisoft (TU Darmstadt, TU München) kann mit den Erfahrungen in der Konstruktion sicherer Systemarchitekturen, wie sie an der TU Dresden vorhanden sind, zusammengebracht werden. Langfristig sollte eine voll formal verifizierte Version des Mikrokerns angestrebt werden. Dafür existieren intensive Erfahrungen an der TU Dresden, die auf Projekten wie VFIASCO (DFG) und ROBIN basieren.

5.1.1.5.5 Interaktion mit neuen HW-Architekturen

Die Gründung des neuen AMD-OSRC (Operating System Research Center) in Dresden ist eine neue und bedeutende Chance für die Hochtechnologienentwicklung in Deutsch-

---

30 Vgl. http://bitkom.de/files/documents/Zukunft_digitale_Wirtschaft_BITKOM-Roland_Berger_Studie.pdf, S. 8.

land und speziell im Raum Dresden. Aufgabe des OSRC ist die Analyse neuer Hardware-Architekturen in Hinblick auf ihre Eignung für moderne Betriebssystemkonzepte. Die neuen Eigenschaften der Hardware in heutigen und nächsten Generationen von Prozessoren können (und sollten) für eine wesentlich bessere und effizientere Unterstützung virtueller Maschinen und sicherer Anwendungen genutzt werden. Eine enge, auch öffentlich geförderte Zusammenarbeit zwischen TU Dresden und AMD OSRC, kann zu einer signifikanten Stärkung von Dresden als einem auch für Informatik-Entwicklung und -Forschung international erstklassigen Standort beitragen. Eine weitere wichtige Frage ist der Umgang mit sog. “Multicore”-Architekturen.

5.1.2 Schwerpunkte und Arbeiten am Horst Görtz Institut für Sicherheit in der Informationstechnik an der Ruhruniversität Bochum

Um die mit der Verbreitung und Nutzung von Informations- und Telekommunikationstechnologien verbundenen sicherheitsrelevanten Fragestellungen in einem umfassenden Ansatz anzugehen, wurde die Forschungskapazitäten auf dem Gebiet der IT-Sicherheit an der Ruhr-Universität Bochum (RUB) unter dem Dach des Horst Görtz Instituts (HGI) zusammengefasst. Das HGI wurde im Jahr 2002 mit erheblicher finanzieller Unterstützung der privaten Horst-Görtz Stiftung mit über 5 Mio. Euro, mit Mitteln der Landesregierung NRW sowie Zuwendungen der EU gegründet.[31]

5.1.2.1 Institutionelle Verankerung

Das HGI ist mit insgesamt etwa 50 interdisziplinär ausgerichteten Wissenschaftlern eine der größten Hochschuleinrichtungen dieser Fachrichtung in Europa. Das HGI deckt nahezu alle Bereiche der modernen IT-Sicherheit ab, insbesondere werden zentrale Fragen der eingebetteten Sicherheit (Embedded Security, Trusted Computing), der theoretischen und angewandten Kryptographie, der Sicherheit in mobilen und festen Telekommunikationsnetzen sowie der Schutz digitaler Inhalte (Enterprise Rights Management, Watermarking) behandelt.

Darüber hinaus ist das HGI einer der drei Initiatoren von ECRYPT, dem European Network of Excellence (NOE) in Cryptography. Hinzu kommt ein Lehrstuhl am Institut für Sicherheit im E-Business (ISEB). Das HGI hat seit seiner Gründung wichtige Konferenzen wie z. B. die AES 4 (Advanced Encryption Standard), CHES 2003 (Cryptographic Hardware and Embedded Systems) und die ECC 2004 (Elliptic Curve Cryptography) organisiert, die erheblich zu seiner internationalen Anerkennung beigetragen haben.

---

31 Vgl. http://www.hgi.ruhr-uni-bochum.de/.

Insgesamt verfügt das HGI über fünf Lehrstühle bzw. Professuren - drei in der Fakultät für Elektrotechnik und Informationstechnik und zwei in der Fakultät für Mathematik -, in denen die Bereiche

- Kryptologie und IT-Sicherheit,
- mathematische und algorithmische Aspekte der Angewandten Kryptologie,
- Kommunikationssicherheit,
- Systemsicherheit sowie
- Netz- und Datensicherheit

behandelt werden.

Daneben existiert das Institut für Sicherheit im E-Business (ISEB), das über weitere sieben Lehrstühle mit einer wirtschaftswissenschaftlichen Ausrichtung verfügt (vgl. Abb. 5-1).

Abbildung 5-1: Organigramm des Horst Görtz Instituts[32]

Aktivitäten zu TC sind vor allem am Lehrstuhl für Systemsicherheit (SysSec) angesiedelt, deren Inhaber derzeit Prof. Dr.-Ing. Ahmed-Reza Sadeghi[33] ist.

32 Vgl. http://www.hgi.rub.de/.

5.1.2.2 Schwerpunkte der Aktivitäten

Die Forschungsschwerpunkte der Applied Data Security (ADS) Arbeitsgruppe am Lehrstuhl für Systemsicherheit bestehen vor allem im

- Entwurf und der Sicherheitsanalyse von kryptographischen Protokollen und TC-Spezifikationen,
- Entwurf von Sicherheitsmodellen und der Sicherheitsanalyse kryptografischer Hardware,
- Entwurf und Implementierung von sicheren Betriebssystemen sowie Trusted Computing Plattformen (Trusted Booting, Remote Attestation, Secure Backups), sowie im
- Entwurf und der Implementierung von Digital Rights Management.

Daneben beteiligt sich der Lehrstuhl an der Organisation eines Aus- und Weiterbildungsangebots und unterstützt als Gesellschafter der gits AG die International School of IT Security (isits).[34] Ferner ist der Lehrstuhl für Systemsicherheit an der Ausrichtung nationaler und internationaler Konferenzen und Workshops wie z. B.

- Western European Workshop on Research in Cryptology (WeWoRC) 2007,
- The secon Workshop on The Second Workshop on Advances in Trusted Computing (WATC‘06 Fall),
- INDOCRYPT 2006,
- First ACM Workshop on Scalable Trusted Computing (STC) 2006,
- First Benelux Workshop on Information and System Security 2006,
- International Workshop on Information Security Applications (WISA) 2006,
- International Workshop on Digital Watermarking (IWDW 2006),
- Financial Cryptography and Data Security (FC) 2006,
- Financial Cryptography and Data Security (FC) 2005,
- SKOLIS Conference on Information Security and Cryptography (CISC) 2005,
- ACM Workshop for Digital Rights Management (ACMDRM) 2005,

---

33 Vgl. http://www.prosec.ruhr-uni-bochum.de.
34 Vgl. https://is-its.org/.

- New Security Paradigm Workshop (NSPW) 2005,
- Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2005,
- Information Security & Hiding (ISH) 2005, at “The International Conference on Computational Science & Its Applications (ICCSA 2005)” beteiligt.

Die Aktivitäten im Bereich TC sowie DRM des HGI sowie des Lehrstuhls für Systemsicherheit sind entsprechend vielfältig. Eine der wichtigsten einschlägigen Tätigkeitsschwerpunkte stellt in den letzten Jahren die Durchführung des Projektes „European Multilaterally Secure Computing Base“ (EMSCB)[35] dar, das 2005 gestartet wurde. Im Rahmen dieses Projektes, das u. a. vom BMWi und den involvierten Firmen finanziert wird, arbeiten als Projektpartner das Institut für Internetsicherheit der Fachhochschule Gelsenkirchen, die TUD, die Sirrix AG, die escrypt GmbH sowie als strategische Partner die Infineon Technologies AG, die SAP AG sowie die Blaupunkt GmbH mit.

Im Rahmen von EMSCB wird eine Plattform entwickelt, die - basierend auf der Trusted Computing Technologie - Hardwarefunktionalitäten, einen Sicherheitskern sowie Funktionalitäten für eine effiziente Migration herkömmlicher Betriebssysteme zur Verfügung stellt. Ziel des Projektes ist es somit, eine aus verschiedenen Einzelmodulen bestehende offene Sicherheitsplattform für Trusted Computing-Anwendungen zu entwickeln. Diese aus den verschiedenen F&E-Aktivitäten resultierenden Einzelmodule sind unter dem Label „TURAYA“ zusammengefasst. TURAYA bedeutet im Kern die Umsetzung der EMSCB-Sicherheitsarchitektur.

TURAYA basiert auf verschiedenen technischen und systemischen Ebenen: Auf der Hardwareebene stellt TURAYA TC-Technologie etwa in Form des TPM zur Verfügung. Auf der nächsten Ebene wird eine Trusted Software (Trusted Software Layer (TSL)) implementiert, die das alleinige Zugriffsrecht auf alle Hardwarefunktionen und -ressourcen besitzt (Ressource Management Layer). Beide Funktionalitäten beschreiben den Security Kernel. Gleichzeitig erweitert die Trusted Software die Schnittstellen der darüber liegenden Betriebssysteme bzw. der damit gesteuerten Anwendungen (Application Layer). Das bedeutet, dass oberhalb der Sicherheitsebene sicherheitsunkritische Anwendungen problemlos parallel zu sicherheitskritischen Anwendungen ausgeführt werden können.

Als Ergebnisse der bisherigen F&E-Arbeiten stehen die Module „TURAYA.Crypt“ sowie „TURAYA.VPN“ zur Einsichtnahme bzw. zum Download zur Verfügung. Während TURAYA.Crypt zur Verschlüsselung von Datenspeichern dient, stellt TURAYA.VPN einen IPSec-VPN-Client dar, der sich zu den handelsüblichen VPN-Servern kompatibel verhält.

---

35 Vgl. http://www.emscb.de.

Zur Branchenmesse CeBIT haben die Akteure des EMSCB-Projektes das „TURAYA.DRM“-Modul vorgestellt, dass die technische Umsetzung des Digital Rights Managements ermöglichen soll. Bis zum Jahresende 2007 soll unter Mitwirkung von SAP das Modul „TURAYA.ERM“ abgeschlossen werden, mit dessen Hilfe das sichere Management von Dokumenten ermöglicht werden soll. In Bearbeitung befindet sich ein weiteres Modul „TURAYA.Embsys“, das in Zusammenarbeit mit dem Konsortialpartner Bosch entwickelt wird.

EMSCB ermöglicht durch seine Funktionalitäten, dass den unterschiedlichen Befürchtungen der Endnutzer, wie sie in Deutschland etwa bis 2004 intensiv diskutiert und artikuliert wurden, begegnet werden kann, in dem der Nutzer jederzeit die volle Kontrolle über die verwendeten Endgeräte, die darauf laufenden Anwendungen sowie seine persönlichen Daten behält. Umgekehrt können durch EMSCB die Rechte an Inhalten gewahrt und der volle wirtschaftliche Nutzen aus ihnen gezogen werden. „Der so entstehende Konflikt zwischen den Interessen und den Sicherheitsanforderungen der Endanwender (Individualdatenschutz und Selbstbestimmung) und den Anbietern von Inhalten und Anwendungen, kann durch eine allseits vertrauenswürdige Computerplattform, die das Gleichgewicht der Interessen garantiert, gelöst werden“.[36]

Die Akteure und Entwickler von EMSCB verweisen darauf, dass das offene Design des L4-Mikrokernels - der kaum mehr als 100.000 Codezeilen enthält – sowie das große Spektrum der Einsatzbereiche, der uneingeschränkte Zugang zu allen Spezifikationen und der freie Zugang zur EMSCB-Plattform als Open Source Lizenz eine wichtige Basis für künftige Geschäftsfelder der (deutschen) IT-Sicherheitsindustrie darstellen.[37]

Zum einen können neue Geschäftsmodelle z. B. im Bereich der Embedded Systems, also etwa im Bereich mobiler Endgeräte, des Maschinenbaus oder Automobilindustrie entwickelt werden. Diese Enwicklungsrichtung ist von immenser wirtschaftlicher Bedeutung, da immer mehr technische Produkte, Maschinen, Netzwerkkomponenten oder Geräte elektronische Steuereinheiten besitzen, deren Verfügbarkeit und Verlässlichkeit heute in vielen Anwendungsbereichen eine kritische Dimension erlangt haben.

Zum anderen kann EMSCB auf der Basis des „Mobile-Trusted-Module“-Standards in beliebigen mobilen Endgeräten (Smart Phones, PDAs, Notebooks, Gaming Konsolen, Barcode Scanner etc.) eingesetzt werden, die in den nächsten Jahren einen erheblichen Bedeutungszuwachs erfahren werden, sei es als Speicher für persönliche Daten, sei als Datenbank, sei es als Zugriffstool auf Geschäftsprozesse oder sei es als elektronische Geldbörse.

---

36 Vgl. http://www.emscb.de/content/pages/Nutzen.htm.

37 Es sei darauf hingewiesen, dass der L4-Mikrokernel als auch die im Rahmen von EMSCB eingesetzte Virtualisierungstechnik lizenziert sind und nicht im Rahmen von EMSCB entwickelt wurden.

Neben der Leitung und Koordination des EMSCB-Projektes ist ADS in folgenden weiteren Projekten engagiert:

- Open TC (Open Trusted Computing),
- PERSEUS,
- TPM Compliance Tests,
- Sokrates (in Zusammenarbeit mit IBM Zürich),
- SECED (Reducing security vulnerabilities in consumer electronic devices using a security-kernel (in Zusammenarbeit mit Philips Research Eindhoven)),
- SPEED (Signal Processing in Encrypted Domain) project, sowie einigen kleineren Projekten wie
- TrustedGRUB, Secure GUI, Secure Application Manager, Trusted Viewer und Linux TPM Driver.[38]

5.1.2.3 Vernetzung mit anderen Akteuren

Die Aktivitäten des HGI sind eingebettet in den institutionellen Verbund mit dem 2001 als Public Private Partnership gegründeten Europäischen Kompetenzzentrum für IT-Sicherheit an der Ruhr-Universität Bochum (eurobits e. V.), um Grundlagenforschung sowie angewandte F&E mit einander zu verbinden. Um einen möglichst effizienten Brückenschlag zwischen Grundlagenforschung sowie angewandter Forschung zu implementieren und um die Nachfrage auf dem Gebiet der IT-Sicherheit bedienen zu können, wurden zwei Forschungsinstitute und weitere drei hochspezialisierte Firmen auf dem Gebiet der IT-Sicherheit integriert.[39]

Insofern bestehen seitens des HGI sowie des Instituts für Sicherheit im E-Business (ISEB) enge Verbindungen zur Gesellschaft für IT-Sicherheit (gits AG),[40] zur escrypt GmbH sowie zur GITS Projekt GmbH Projektgesellschaft für IT-Sicherheit, die sich mit Trainings- und Weiterbildungsaktivitäten, mit angewandter Forschung und Entwicklung, mit Technologietransfer, mit Embedded Security und allgemeinen Projektmanagementdienstleistungen befassen.

eurobits e. V. hat seit seinem Bestehen ein internationales Netzwerk mit Kooperationspartnern sowohl aus der Industrie als auch der Wissenschaft aufgebaut, das nicht nur in

---

38 Vgl. http://www.prosec.trust.rub.de/activities.html.
39 Vgl. http://www.eurobits.de.
40 Die gits AG wird finanziell unterstützt durch die Europäische Union sowie das Land NRW.

den meisten europäischen Ländern, sondern auch in Nordamerika (Kanada, USA), Südamerika (Brasilien, Chile), Asien (China, Japan, Indonesien, Malaysien) sowie in Australien beheimatet ist. Zu den Kooperationspartner gehören u. a.

- BSI,
- ECRYPT,
- Euler Institute for Discrete Mathematics and ist Applications (EIDMA),
- AutoUni,
- Blaupunkt/Bosch,
- BMW,
- DaimlerChrysler,
- IBM T.J. Watson Labs (USA),
- Infineon,
- NEC Networks Labs,
- Nokia,
- Sun Labs (USA),
- Telekom AG,
- Philips,
- Rohde&Schwarz,
- Vodafone,
- Volkswagen.

Zu den weiteren wichtigen Partnern des HGI sowie des Lehrstuhls für Systemsicherheit gehört die Sirrix AG security technologies.[41] Die Sirrix AG ist ein Spin-off Unternehmen der Universität des Saarlandes sowie des Deutschen Forschungszentrums für Künstliche Intelligenz (DFKI) und verfügt über einen Firmensitz jeweils in Saarbrücken sowie in Bochum.

---

41 Vgl. http://www.sirrix.de/content/pages/home.htm.

Zu den Kompetenzbereichen der Sirrix AG gehören u. a. der Entwurf, die Analyse und die Entwicklung kryptografischer Protokolle und Verfahren. Besondere Aktivitäten, die direkt TC (Security Kernels, Secure Operating Systems) betreffen, wurden bzw. werden durch eine Kooperation im Rahmen des Projektes PERSEUS entwickelt.[42]

Die Sirrix AG ist Mitglied der TCG, von eurobits e. V. sowie des Firmenzusammenschlusses IT-Security Made in Germany (ITSmiG), der ebenfalls vom BMWi gefördert wird. Kooperationen bestehen u. a. mit der Fraunhofer Gesellschaft (FhG), dem Fraunhofer Institut für Sichere Informationstechnologie (SIT), der TUD, der T-Mobile Stiftungsprofessur für M-Commerce (Frankfurt) und dem renommierten New Yorker STEVENS Institute of Technology (Hoboken).

Als weiterer wichtiger Partner im Netzwerk ist das European Network of Excellence (NoE) in Cryptography (ECRYPT) zu nennen, dessen Gründungsmitglied das HGI ist. ECRYPT umfasst mehr als 30 Kryptogruppen aus Hochschulen und Industrie, deren Forschungsschwerpunkte durch das HGI koordiniert werden.

5.1.3 Schwerpunkte und Arbeiten am Institut für Internet-Sicherheit an der Fachhochschule Gelsenkirchen

Mit dem Bedeutungszuwachs des Internet und auf Grund seiner Schlüsselrolle für die moderne Gesellschaft wurde an der Fachhochschule Gelsenkirchen im Jahr 2005 das Institut für Internet-Sicherheit – if(is)[43] – gegründet. Mit dem Fachbereich Informatik, der derzeit insgesamt 19 Professuren umfasst, werden Kernkompetenzen in den Bereichen

- 3D Messtechnik,
- Softwarentwicklung,
- Smart Materials,
- Unternehmenswachstum, sowie
- Internet-Sicherheit

abgedeckt. if(is) verfügt über zwei Professuren und beschäftigt über 30 Mitarbeiter. Die Professur für Internet-Sicherheit hat Prof. Dr. Norbert Pohlmann inne, der gleichzeitig Direktor des if(is) ist.[44]

---

42 Vgl. http://www.perseus-os.org/content.htm.
43 Vgl. http://www.ifis-fhm.de/ sowie Pohlmann 2005.
44 Vgl. http://internet-sicherheit.de/.

5.1.3.1 Institutionelle Verankerung

Das Institut für Internet-Sicherheit ist eine Fachbereichs-übergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Übergeordnete Aufgabenstellung des Instituts ist es, die Forschung und Entwicklung auf dem Gebiet der Internetsicherheit und deren rechtliche Rahmenbedingungen voran zu treiben sowie die wissenschaftliche Grundlegung und Weiterentwicklung der anwendungsbezogenen Lehre im Bereich der Internetsicherheit zu vertiefen. Zu diesen Aktivitäten gehören insbesondere

- die Entwicklung und Durchführung von einschlägigen Lehrveranstaltungen,
- die Entwicklung und das Angebot von Weiterbildungsveranstaltungen, Kongressen und Workshops,
- die Durchführung von Forschungs-, Beratungs- und Entwicklungsvorhaben in Kooperation mit anderen Hochschulen sowie Industrieunternehmen.

5.1.3.2 Schwerpunkte der Aktivitäten

Seit seiner Gründung hat ifis eine bedeutende Zahl von Forschungsthemen bearbeitet und seine Kompetenzen im Bereich der Ausbildung kontinuierlich ausgeweitet.[45] Daneben hat sich ifis zur Aufgabe gemacht, Beratungsleistungen für öffentliche Hände sowie Industrieunternehmen anzubieten. Seine allgemeinen Schwerpunkte in der Lehre, der Forschung sowie der Beratung im Bereich Internet-Sicherheit sind

- Internet-Frühwarnsysteme, IT-Frühwarnsysteme,
- Internet-Analyse-Systeme,
- Verfügbarkeit der Dienste im Internet,
- Wissenschaftliche Grundlagen zur Auswertung von Internet-Messdaten,
- Anti-Spam (Konzepte, Umsetzungsstrategien, empirische Untersuchungen),
- Digitale Signatur und Verschlüsselung, Virtuelle Poststelle,
- Password Fishing (Aufklärungs- und Erkennungsstrategien),
- Harvesting (Forschung), sowie
- Viren, Würmer, Trojaner (Erkennungsstrategien im Internet).

---

45 Vgl. http://www.internet-sicherheit.de/institut.html.

Daneben hat if(is) zentrale Schwerpunkte in seiner Arbeit gesetzt und verfolgt u. a. Aktivitäten in den nachfolgend skizzierten Bereichen.

E-Mail Sicherheit

Anti-SPAM (Konzepte, Umsetzungsstrategien, empirische Untersuchungen) Viren (Konzepte, Umsetzungsstrategien, empirische Untersuchungen).

Internet-Statistik-System

Das Ziel des Internet-Statistik-Systems ist es, kommunikationstechnische, anwendungsrelevante und sicherheitsorientierte Informationen (Statistiken, Profile, Ist-Zustand, Alarme, Vorhersagen) aus dem Internet zu gewinnen, um verlässlichere Planung und schnellere Reaktionszeiten auf unerwünschte Zustände des Internets zu ermöglichen.

XKMS

Die XML Key Management Specification definiert ein Protokoll, um die Validierung und Verwaltung von Schlüsseln auf XML Basis via Web-Services zu verwirklichen. Die resultierenden Vorteile vereinfachen den Umgang mit der PKI wesentlich. ifis hat ein solches System entwickelt und testet es auf Praxistauglichkeit. Die resultierenden Vorteile machen den Umgang mit einer PKI einfacher und schlanker.

Identity Management

„Einheitliche“ Identifikations- und Authentikationsverfahren im Internet. Themen in diesem Bereich sind u. a. einheitliche Authentifikationsverfahren auf der Basis von PKIs, Single Sign On, Liberty Alliance (Global LogIn, Circle of Trust).

Sicheres Chatten im Internet

In diesem Arbeitsschwerpunkt wurde ein Chatsystem entwickelt, welches eine sichere Kommunikation und einen sicheren Betrieb gewährleistet. Ein besonderer Schwerpunkt ist die vertrauenswürdige Gestaltung der Benutzerschnittstellen, die eine diskrete Chatberatung im professionellen Bereich, wie z. B. der psychologischen Beratung ermöglicht.

Kommunikationsaspekte

Die Notwendigkeit über Netzwerke zu kommunizieren wird durch die Umsetzung moderner IT-Konzepte in der Zukunft noch viel umfänglicher und flexibler notwendig sein.

Wichtige Forschungsaktivitäten bestehen daher im Bereich Verteilte Systeme, Mobilanwendungen sowie Ubiquitous- oder Pervasive-Computing.

Faires Digital Right Management (DRM)

Aus Sicht des ifis besteht das Ziel von fairen DRM-Systemen darin, geeignete Umgebungen und Rahmenbedingungen für die Nutzung digitaler Werke zu schaffen, so dass die Interessen und Sicherheitsanforderungen aller beteiligten Parteien in sinnvoller Weise berücksichtigt werden. Somit sollen faire DRM-Methoden im allgemeinen für einen Vertragsabschluss und dessen Einhaltung sorgen.

IP Telefonie (Voice over IP)

In diesem Bereich beschäftigt sich ifis mit Quality of Service Anforderungen und neuen Abhängigkeiten auf Grund des Abbaus alter Strukturen. Außerdem wird das Thema ‚Spam im Bereich IP-Telefonie' behandelt.

Mobile Netze

Im Bereich der Mobilen Netze geht es um WLAN- und Bluetooth-Sicherheit sowie um die sichere Integration von mobilen Nutzern in bestehende Unternehmensnetze wie z. B. der Möglichkeiten der Zugangssicherung, der verschlüsselten Kommunikation usw.

Trusted Computing

Kooperation mit den Teilnehmern des Forschungsprojektes EMSCB zur Entwicklung einer vertrauenswürdigen, fairen und offenen Sicherheitsplattform basierend auf der Trusted Computing Technologie.

Internet-Recht

Im Themenfeld Internet-Recht geht es um die rechtlichen Rahmenbedingungen und Möglichkeiten des geschäftlichen Handelns im Internet. Hierzu zählen insbesondere die Themenbereiche

- Anpassung und Flexibilität der anwendbaren Rechtsnormen,
- Gestaltung der Rechtsbeziehungen zwischen den Beteiligten,
- Datenschutz und Recht im E-Commerce, sowie
- Streitschlichtung und Mediation mittels Internet.

Sicherheit in Next Generation Networks

Während es heute Sicherheitslösungen in Netzen gibt, die auf die jeweilige Technologie oder ein spezielles Angebot zugeschnitten sind, wird es in Zukunft wichtig sein, all diese Technologien zu einem Next Generation Network zu verschmelzen. Das Zusammenwachsen dieser verschiedenen Technologien und Angebote bedeutet, dass die Sicherheit in den neuen Dienstleistungen mit neuen Übergängen zwischen Verantwortung und komplexen Beziehungen kontrolliert werden muss. In offenen Systemen sind andere, betreiberübergreifende Lösungskonzepte für funktionierende Sicherheitsmechanismen erforderlich. ifis beschäftigt sich mit den neuen Anforderungen eines Next Generation Networks und entwickelt Strategien und Lösungen mit dem Ziel, einen sicheren und vertrauenswürdigen Betrieb von Informations- und Kommunikationstechnik zu schaffen.

Branchenbuch IT-Sicherheit

Das Branchenbuch IT-Sicherheit ist die erste deutsche neutrale und nicht kommerzielle Plattform, die das Finden von Sicherheitslösungen erleichtert. Firmen erhalten im Branchenbuch IT-Sicherheit die Möglichkeit, Referenzen anzugeben. Der Suchende erhält einen umfassenden Überblick über das Angebot und eine Orientierungshilfe bei seiner Entscheidung, welcher Anbieter zu ihm passt. Mit Hilfe von Anwenderberichten und Referenzen kann der potentielle Kunde ein hohes Vertrauen entwickeln. Das Branchenbuch kommt ihrem Bedürfnis nach, Dienstleister in der Region zu finden, in der sie selbst ansässig sind.

5.1.3.3 Vernetzung mit anderen Akteuren

ifis ist nicht nur durch seine Aktivitäten im Bereich Lehre sowie F&E und Beratung, sondern auch durch seine institutionellen und organisatorischen Bezüge sowohl im nationalen Bereich als auch im internationalen Umfeld vernetzt. Dazu tragen u. a. Konferenzen und Workshops bei, die ifis organisiert und bei denen das Institut mitwirkt. U. a. zeigt dies auch die Zusammensetzung des Institut-Beirates, der mit Führungskräften aus renommierten Institutionen und Unternehmen (Bundesamt für Sicherheit in der Informationstechnik, Lucent GmbH, secunet Security Networks AG, T-Online International AG) besetzt ist.

ifis gehört ferner dem Kompetenzverbund „Competence Center for Internet Security“ an, der gemeinsam für mehr Sicherheit und Vertrauenswürdigkeit im Internet sorgen will. Außerdem fördert der Kompetenzverbund die wissenschaftlichen Aktivitäten des Institutes für Internet-Sicherheit.

Durch seine regionalen Bezüge entfaltet ifis auch Aktivitäten auf Länderebene und ist an der NRW-Initiative “secure IT“ beteiligt.

5.1.4 Schwerpunkte und Arbeiten am Fraunhofer-Institut für Sichere Informationstechnologie (SIT)

Die Fraunhofer-Gesellschaft (FhG) gehört zu den führenden Organisationen für angewandte Forschung in Europa. Sie betreibt anwendungsorientierte Forschung für Industrieunternehmen, Dienstleistungsunternehmen sowie für öffentliche Institutionen und finanziert rund zwei Drittel ihrer Forschungsaufträge durch das Einwerben von Drittmitteln. Die rund 56 Fraunhofer-Institute in Deutschland sind auf über 40 verschiedene Standorte verteilt und verfügen über rund 12.500 Mitarbeiter.

Das Institut mit Bezug zu Fragen der IT-Sicherheit bzw. zu Trusted Computing ist das Fraunhofer-Institut für Sichere Informationstechnologie SIT in Darmstadt, das auf Grund der Ausrichtung der Fraunhofer-Gesellschaft einen besonders hohen Anwendungsbezug der von ihm verfolgten Lösungen im Blick hat und seine F&E-Aktivitäten generisch auf Bedürfnisse von Auftraggebern ausrichtet.[46]

5.1.4.1 Institutionelle Verankerung

Ende 2005 arbeiteten am Fraunhofer-Institut für Sichere Informationstechnologie SIT 73 wissenschaftliche Angestellte. Auf Grund dieser personellen Ausstattung kann Fraunhofer SIT alle Bereiche der IT-Sicherheit abdecken und ist dementsprechend für Unternehmen aller Branchen tätig. Die Leitung von Fraunhofer SIT liegt in den Händen von Frau Prof. Dr. Claudia Eckert, die zugleich eine Professur am Fachbereich Informatik FG Sicherheit in der Informationstechnik der Technischen Universität Darmstadt bekleidet.

5.1.4.2 Schwerpunkte der Aktivitäten

Das Fraunhofer-Institut SIT befasst sich mit vielen wichtigen Aspekten der IT-Sicherheit und hat in den vergangenen Jahren umfangreiche Kernkompetenzen entwickelt, die sich auf folgende Bereiche erstrecken:

- Sicherheitsmanagement
  Sicherheitsanalysen, Sicherheitskonzepte, Entwicklung von Werkzeugen für das Risiko-Management, Modellierung von Sicherheitsarchitekturen,

- Gestaltung von Sicherheit im praktischen Betrieb von Systemen
  Sichere IT-Infrastrukturen, Sicheres Rechenzentrum, Firewalls, VPN, Intrusion Detection, Virenschutz,

---

46 Vgl. http://www.sit.fraunhofer.de/.

- Gestaltung Elektronischer Geschäftsprozesse Analyse und Umstrukturierung von Geschäftsprozessen, Absicherung sicherheitskritischer Prozesse, Einsatz von sicheren elektronischen Diensten,
- Gestaltung sicherer Mobilität, nahtlose Dienstnutzung, Optimierung mobiler Geschäftsprozesse, Entwicklung vertrauenswürdiger Diensteplattformen, Sicherheit und Schutz mobiler Netzwerkinfrastrukturen,
- Schutz von Inhalten und Werten, DRM-Systeme, Zugriffsschutz (RBAC), Content-Sicherheit und Langzeitarchivierung elektronisch signierter Dokumente, Digitale Signatur, Verschlüsselungstechniken,
- Sichere und vertrauenswürdige Identifikation, Smartcards, Biometrie, RFID, Public-Key-Infrastrukturen (PKI), Single-Sign-On (SSO), Verzeichnisdienste,
- Implementierung von Sicherheit, Revocation (von Schlüsseln oder Zertifikaten) und Integration von Verzeichnisdiensten, Erhaltung von Interworkingfähigkeit, Verbesserung der Benutzerakzeptanz,
- Bewertung und Prüfung von Sicherheit, Entwicklung formaler Methoden (APA und Abstraktionen) und Tools, Spezifikation, Verifikation, Validierung, Simulation und Visualisierung von Systemen.

Neben diesen allgemeinen F&E-Schwerpunkten hat Fraunhofer SIT in den letzten Jahren – meist eingebettet in die Kooperation mit Partnern aus der Industrie - zahlreiche Projekte bearbeitet wie z. B.

5.1.4.2.1 *Sicherheit für die ubiquitäre Internetnutzung*

Die Vision von SicAri besteht in der Entwicklung einer Sicherheitsplattform, um Internetanwendungen zu jeder Zeit an jedem Ort und mit jedem Gerät sicher nutzen zu können. Hierzu wird ein modularer Werkzeugkasten für Sicherheitsdienste und eine integrierende Sicherheitsplattform entwickelt. Die SicAri-Plattform ist die Kontaktstelle für den Benutzer, ob unterwegs, zu Hause oder an seinem Arbeitsplatz. Sie bietet dem Benutzer Dienstleistungen an, die sich in Basisdienste und Applikationsdienste unterteilen lassen. Im Fokus der Arbeiten stehen hierbei Sicherheitspolitiken, die alle sicherheitsrelevanten Entscheidungen regeln.

Transi§Doc: Rechtssichere Transformation signierter Dokumente

Damit elektronische Signaturen prüfbar bleiben, dürfen die signierten Daten nicht verändert werden. Solche Veränderungen treten aber zwangsläufig auf, wenn Daten beim Austausch in vernetzten Systemen oder bei der Migration von Systemen konvertiert werden. Ziel des Projekts TransiDoc ist es daher, Verfahren zu entwickeln, um signierte

Dokumente so zu konvertieren, dass ihr Beweiswert und andere rechtlich wesentliche Eigenschaften erhalten bleiben (rechtssichere Transformation). Ausgehend von Anwendungsbeispielen in Kommunalverwaltung, Gesundheitswesen und Notariat soll das Projekt rechtliche und technische Anforderungen analysieren, praktikable Konzepte für technische und organisatorische Verfahren entwickeln, Demonstratoren und Prototypen implementieren sowie Erkenntnisse durch Tests und eine Simulationsstudie evaluieren.

secure-it.nrw.2005

Das Bundesland Nord-Rhein-Westfalen (NRW) hat mit der „secure-it.nrw.2005“ Initiative die IT-Sicherheit im elektronischen Geschäftsverkehr gefördert. Dabei sollte die Öffnung insbesondere von kleinen und mittleren Unternehmen, aber auch der öffentlichen Verwaltung für E-business gestärkt und das Vertrauen der Anwender in die Sicherheit der Informationstechnik erhöht werden.

5.1.4.2.2 *PasswordSitter:* Flexibles webbasiertes Passwort-Management

Der PasswordSitter vom Fraunhofer-Institut SIT löst zahlreiche Passwortprobleme. Er sorgt für starke Passwörter und liefert sie sicher auf jedes Gerät. Der Password-Sitter ermöglicht Unternehmen, ihre Mitarbeiter zu entlasten, die Helpdesk-Kosten zu senken, Produktivitätsausfälle zu vermeiden und die Sicherheit des eigenen Unternehmens deutlich zu erhöhen.

5.1.4.2.3 Mobile Sichere Dienste für mobile Bürger

Bei diesem Projekt geht es um eine Plattform für mehrseitig sichere, profilgesteuerte Dienste am Beispiel touristischer Location-Based Services. Neben der Ausfallsicherheit von Netzen und Diensten bietet die Mobile-Plattform ein vertrauenswürdiges Agentensystem, Plattform-gerechte Darstellung und lässt sich durch weitere Dienste ergänzen.

5.1.4.2.4 ArchiSoft Langzeitsicherung elektronisch signierter Dokumente

Bei ArchiSoft steht eine Lösung für die sichere und den Beweiswert erhaltende Langzeitarchivierung von elektronisch signierten Dokumenten im Mittelpunkt. Mit ihr können Unternehmen nicht nur gesetzliche Archivierungsauflagen erfüllen, sondern auch die eigene Archivierung erheblich rationalisieren. Zudem lässt sich ArchiSoft leicht in Dokumenten-Management-Systeme integrieren.

5.1.4.2.5 *SHVT Simple Homomorphism Verification Tool*

SHVT Simple Homomorphism Verification Tool stellt ein Werkzeug zur Unterstützung des kompletten Zyklus von der Spezifikation bis zur Evaluierung von kooperierenden Systemen dar. Es enthält einen grafischen Editor zur Spezifikation, einen Simulator und eine Komponente zur Analyse und Visualisierung des dynamischen Systemverhaltens sowie zur Berechnung von Abstraktionen des Systemverhaltens.

5.1.4.2.6 eSI Der elektronische Sicherheitsinspektor

Bei eSI handelt es sich um ein Werkzeug zur automatischen Suche von Sicherheitslücken. Der elektronische Sicherheitsinspektor (eSI) überprüft, ob die Vorgaben des jeweiligen Sicherheitskonzepts auch tatsächlich eingehalten werden.

5.1.4.2.7 Flexhaus Gebäude als Anbieter von Diensten

Im Mittelpunkt von Flexhaus steht eine Gebäudekonzept für die variable Nutzung von Räumen unter Nutzung des Raumcomputers zur einheitlichen Steuerung sämtlicher Haussysteme.

5.1.4.2.8 NSI Neue Sicherheitsstrukturen für das Internet

In diesem Projekt geht es um Lösungen für die bessere Benutzbarkeit und Effizienz von vernetzten Public-Key-Infrastrukturen (PKIs).

Über diese konkreten Projektaktivitäten hinaus vergibt Fraunhofer SIT regelmäßig Diplomarbeiten u. a. zu Themen wie: Trusted Computing Security for Web-Browsers, Trusted Ticket Systems oder Trusted Seals for Processes.[47]

5.1.4.3 Vernetzung mit anderen Akteuren

Auf Grund seiner Ausrichtung engagiert sich Fraunhofer SIT im Rahmen von Konferenzen und Workshops für den Wissenstransfer insbesondere in die Wirtschaft. U. a. werden Intensivseminare zum IT-Sicherheitsmanagement, zu Angriffsmethoden und Abwehrstrategien sowie zu IT-Sicherheitskonzepten durchgeführt. Durch Niederlassungen in verschiedenen europäischen Ländern, in den USA sowie in Asien und im Nahen Osten wurde die Zusammenarbeit mit internationalen Partnern institutionalisiert und auf einen kontinuierlichen Austausch hin angelegt.

---

47 Vgl. http://www.sit.fraunhofer.de/cms/de/karriere/_karriere_offene_stellen_1.php.

5.1.4.4 Projektvorschläge zu Forschung und Entwicklung von Trusted Computing-Lösungen

Um den Transfer von TC-Know how in die Wirtschaft zu verbessern, hat Fraunhofer SIT eine Reihe von anwendungsorientierten Projektvorschlägen entwickelt, die im Falle einer Förderung in enger Kooperation mit der Wirtschaft realisiert werden sollen. Zu diesen Projektvorschlägen zählen u. a.

- Qualifizierte Signaturen auf TC-basierten Plattformen

Für die Erzeugung qualifizierter Signaturen wird ein bestimmtes Maß an Vertrauen in die Umgebung verlangt, durch die diese Signaturen erstellt werden. Wichtige Anforderungen stellen sich beispielsweise im Bereich der korrekten Repräsentation des zu signierenden Dokumentes. Verschiedene Konzepte die innerhalb der TCG spezifiziert werden können die Basis für PCs stellen, in die ein hinreichendes Maß an Vertrauen gelegt werden kann. Dieses Konzept reduziert die Kosten für qualifizierte Signaturen im Bereich der Endgeräte und öffnet dieser Technologie den Weg in einen breiten Einsatz wie innerhalb von Web Service Architekturen, aber auch im täglich Gebrauch der Benutzer vor Ort.

- Vertrauenswürdige Siegel für automatisierte Abläufe

Der Umgang mit Dokumenten in (räumlich verteilten) Arbeitsabläufen findet auf vielen verschiedenen Plattformen und Umgebungen statt. Es gilt hierbei meist den Nachweis zu führen, wer wann was auf welchem Gerät gemacht hat, und ob dieses sicher war. Leider fehlt dieser Nachweis meist, so dass eine Überprüfung im Ablauf und später nicht möglich ist. Ein um Trusted Computing erweitertes Model bietet Informationen über den Systemzustand bei Ausführung eines Arbeitsschrittes durch Attestierung und integriert diese in abgesicherte Datenstrukturen. Besonders im Kontext von automatisierten Arbeitsabläufen können wichtige zusätzliche Daten hierdurch dokumentiert werden.

- Maschinensignaturen

Das Anbringen von Signaturen durch Maschinen als beispielsweise Herkunfts- bzw. Ursprungsnachweis digitaler Daten wie Fotos, Videos, gescannter Dokumente oder Ablaufprotokolle wird in verschiedenen Umgebungen bereits heutzutage praktiziert. Es ist allerdings hierbei keine Aussage über den Zustand oder die Identität des Gerätes gegeben, die sich auf eine zertifizierte Hardwarebasis zurückführen lässt. Ziel ist es, eindeutige Bindung an ein bestimmtes Gerät durch TC-Unterstützung zu erreichen. Diese Informationen können durch Zusatzdaten, wie elektronische Signaturen oder Watermarks verfügbar gemacht werden. Solche Maschinensignaturen, die auf einer TC-gesicherten Umgebung basieren, haben das Potential ein deutlich höheres Schutzniveau als konventionelle Ansätze bei niedrigeren Kosten zu bieten.

- Machine-to-Machine Kommunikation

In verschiedenen Umgebungen der Fernwartung und Telemetrie müssen Maschinen untereinander autonom sensitive Daten austauschen. Gleiches gilt grundsätzlich für den Zugang mobiler Endgeräte zu Kommunikationsnetzen. Hierbei werden vertrauenswürdige Kommunikationsendpunkte für die sichere Datenübertragung benötigt. Vertrauenswürdige Maschinen erlangen in diesen Szenarien Zugang zu Kommunikationsnetzen oder Resourcen. Ein weiterer wichtiger Aspekt ist eine sichere Zeitbasis, die zum Beispiel für Abrechnugszwecke erforderlich ist und auch in dezentralen Szenarien zur Verfügung stehen muss.

- Vertrauenswürdiges E-Mail Archiv

Durch verschiedene auch internationale Regulierungen wie Basel II, IFRS oder SOX werden Firmen und Behörden zur Archivierung ihrer auch digitalen Kommunikation verpflichtet. Das Ziel hierbei ist es im Nachhinein Vorgänge revisionssicher darstellen zu können. Eine kosteneffiziente und skalierbare Realisierung ist hierbei von zentraler Bedeutung.

Die Verwendung eines Hardwaresicherheitsankers auf der Basis von Trusted Computing ermöglicht die Realisierung einer Appliance-Lösung. Hierbei wird die Funktionalität durch ein dediziertes System zur Verfügung gestellt, dass die Archiv- und Sicherheitsfunktionalität als ein Modul isoliert. Für dieses Modul können Aussagen über die Sicherheit und Integrität des einzelnen Moduls getroffen werden.

Die Verwendung von Zeitstempeln für die Fixierung des Archivierungszeitpunktes ebenfalls innerhalb des Moduls wird möglich durch eine Referenz auf eine akkreditierte Entität, die diese Zeitstempel ausgibt.

- Trust4VoIP

Trust4VoIP zielt auf die Sicherheit internetbasierter Sprach- und Multimedia-Kommunikation. Kern ist ein völlig neuartiges Verfahren, um solche Kommunikationsdaten digital und in Echtzeit zu signieren. Aufbauend auf diesem innovativen Ansatz werden im Projekt mehrere Anwendungen bis zur Praxisreife entwickelt und getestet. Hierbei stehen mehrere Anwendungsszenarien, die von der Benutzerauthentisierung, über die vertrauenswürdige Archivierung bis zum Signierterminal für Telefonie reichen, im Fokus des Projektes. Ein besonderes Gewicht hat die Behandlung ganzheitlicher Prozessketten und die Verträglichkeit entsprechender Methoden mit den Anforderungen des Daten- und Verbraucherschutzes. Da in Inbound-, Outbound- und Backoffice-Projekten potentiell Gesprächsaufzeichnungen zur Beweissicherheit erfolgter Vertragsabschlüsse, -änderungen oder -kündigungen vorgenommen werden, ergibt sich ein Mehrwert für die Anwendungspartner aus dem CRM-Provider- und Callcenterbereich. Neben der reinen Archivierung von Kommunikation bedeutet eine verbesserte und sich

über das gesamte Gespräch erstreckende Benutzerauthentisierung besonders in mobilen Anwendungen einen deutlichen Sicherheitsgewinn bei verbesserter Verwendbarkeit.

- Trust4IdM

Identitäten von Benutzern haben sich zu einem essentiellen Element in heutigen Systemen entwickelt, da sie auf diesen moderne Regularien wie SOX oder Basel II basieren und durch den Gesetzgeber gefordert werden. Das Vertrauen in diese Identitäten basiert auf dem grundsätzlichen Vertrauen in die Infrastrukturen, die diese Identitäten erzeugen, verwalten und verwenden.

Identitätsmanagement (IdM) kann in besonderer Weise von den Schutzeigenschaften von Trusted Computing profitieren. Die Verwendung von Benutzercredentials, an die die Identitätsaussage gebunden ist, kann auf bestimmte und bekannte Geräte gebunden werden, so dass dieses Credential nur in Verbindung mit dem entsprechenden Endgerät verwendet werden kann. Hierbei kann beispielsweise die Präsenz des Benutzers bei der Verwendung der Credentials gefordert werden.

Des Weiteren kann eine Dezentralisierung der IdM Funktionen in die Endgeräte ermöglicht werden, was zu einer Entlastung zentraler Strukturen beitragen und zu einer Kostensenkung hierfür führen kann. Auch kann ein höheres Vertrauen in die Kommunikation zwischen IdM Domänen erreicht werden, da die Identität und Integrität der beteiligten Entitäten verifizierbar ist und als Basis für ein Vertrauen zwischen den Domänen verwendet wird.

Das Ziel dieses Projektes ist es die Sicherheit und Vertrauenswürdigkeit in Geschäftsprozessen die über die tradierten Vertrauensdomänen hinaus gehen zu erhöhen und damit die Basis zu legen, Partner eng in ihren Arbeitsabläufen zu verzahnen. Konzepte wie „Identity as a Service“ benötigen eine solide Sicherheitsinfrastruktur und schaffen neue Anwendungsszenarien und Geschäftsfelder.

- Trust4DVB

Digital Video Broadcasting (DVB) ist in der Zwischenzeit weit verbreitet und bildet in ganz Europa die Basis für verschiedene kommerzielle Anwendungen wie PayTV aber auch Datendienste, die über IP over DVB ihre Kunden erreichen. Die Inhalte werden hierbei durch den Commen Scrambling Algrorythmen (CSA) geschützt, der die erforderlichen Credentials aus einer Smart Card erhält. Diese SmartCard mit den darin manifestierten Algorithmen benötigt bei verschiedenen Anbietern unterschiedliche Hardware, die im Falle eines Sicherheitsbruchs ausgetauscht werden muss. Ein solcher Austausch der Hardware ist meist für die Anbieter und Kunden mit hohen Kosten verbunden. Bei einem gleichzeitigen Abonnement von mehreren Anbietern, muss bei einem Kanalwechsel auch die Smart Card gewechselt werden, was für den Kunden mit negativen Produktempfinden verbunden wird.

Trusted Computing bietet die Basis die Hardware zu konsolidieren und schafft die Plattform für softwarebasierte Systeme in denen gleichberechtigt Credentials von verschiedenen Anbietern verwaltet werden können. Dies führt zu einer starken Vereinfachung der eingesetzten Set-Top Boxen und ermöglicht einen stärkeren Wettbewerb zwischen den Anbietern.

Zudem wird eine preiswerte Rückkopplung der Hardware mit dem Anbieter oder anderen Entitäten möglich, so dass neue Zahlungsmethoden und Protokolle ermöglicht werden. Dies ermöglicht eine höhere Universalität der Set-Top Box. Entsprechende Konzepte werden in anderen europäischen Ländern bereits angedacht und haben sich in verschiedenen EU Anträgen bereits niedergeschlagen.

- MediTrust

In vielen Bereichen werden durch den Gesetzgeber Dokumentationspflichten vorgegeben, durch die ein Nachweis bestimmter Maßnahmen erfolgt. Besonders in der medizinischen Versorgung von Patienten legt der Gesetzgeber den Ärzten, Pflegern und anderen involvierten Parteien eine Dokumentationspflicht auf.

Verschiedene Prozesse bzw. Abläufe müssen in der stationären wie auch ambulanten Pflege durch das medizinische Personal erfasst und durchgeführt werden. Hierbei muss zum einen die korrekte Durchführung verschiedener Tätigkeiten die sich aus den Hygienevorschriften wie auch aus dem Medizinproduktegesetz ergeben. Medienbrüche kommen häufig in der täglichen Praxis vor und erschweren die Durchführung der Pflege und der Dokumentation, was zu erhöhten Kosten und Zeitaufwendungen führt.

Da diese Verfahren papierbasiert sind können diese Dokumentationen nachträglich angefertigt und auch verfälscht werden. Software- und Hardwaresysteme können helfen in der Pflege in den Aspekten der Vorbereitung und Dokumentation einheitliche und preiswerte Lösungen zu etablieren, die die geforderte Nicht-Abstreitbarkeit liefern. Dokumentationsverfahren und Zeitstempel können bestimmte Maßnahmen am Patienten dokumentieren und zeitlich zuordenbar machen. Eine Kombination aus geeigneten Systemen wie RFID, GPS oder Photografie kann auch den physischen Besuch und den Gesundheitszustand erfassen und damit dokumentieren.

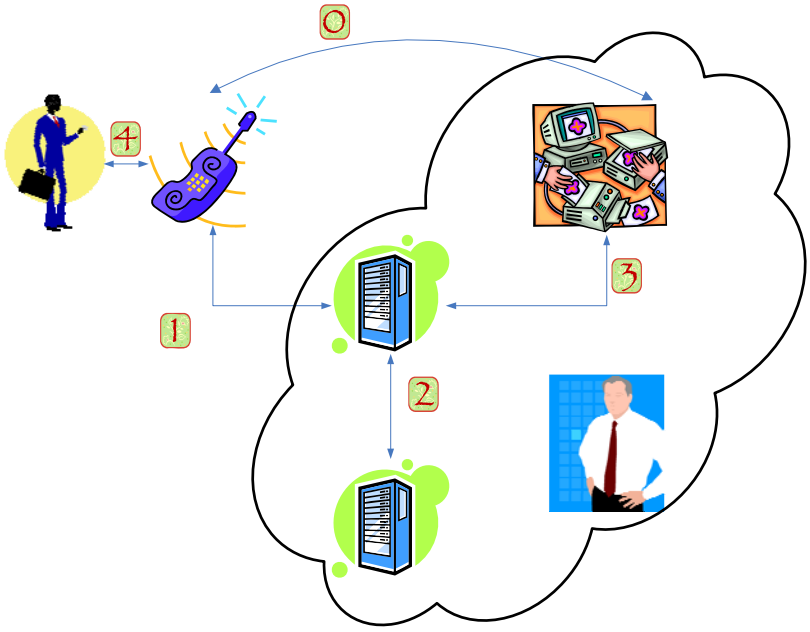
- TrueConnect

Mit der steigenden Funktionalität mobiler Endgeräte wächst auch das Sicherheitsrisiko bezüglich einer möglichen Infektion durch Schadsoftware. Es gibt zwar verschiedene Sicherheitslösungen im Bereich mobiler Anwendungen und Netze, allerdings sind viele dieser Lösungen proprietär und behandeln häufig nur einen bestimmten Sicherheitsaspekt (Verschlüsselungssoftware, Virenschutz, mobiles VPN). Es fehlen Mechanismen, die die Durchsetzung der Sicherheitsrichtlinien von Firmen in den Endgeräten fordern

und deren Existenz überprüfen. Hierzu gehören auch Mechanismen die eine sichere Distribution von Security Policies in Netzen mobiler Endgeräte ermöglichen.

Als Basis zur Problemlösung sind die Mechanismen/Spezifikationen der Trusted Computing Group[48] vorgesehen, insbesondere Trusted Network Connect (TNC). Mittels TNC kann sich ein mobiles Endgerät beim Server/Backend als „vertrauenswürdig“ authentifizieren. TNC dient zur Durchsetzung von Security Policies auf Endgeräten (Prüfung der Aktualität des Betriebssystem-Patchlevels, Virenscanners, Desktop Firewall). Im Falle, dass das Endgerät nicht konform zu den Sicherheitsrichtlinien ist, wird es in eine Quarantänezone isoliert, mit der Möglichkeit, die fehlenden Sicherheitspatches herunter zu laden. Dies stellt sicher, dass alle Endgeräte eine aktualisierte und den Security Policies entsprechende Sicherheitssoftware installiert haben.

Abbildung 5-2: Skizze der TNC-Architektur



48 www.trustedcomputinggroup.org.

Abbildung 5-2 zeigt die beabsichtigte Lösungsarchitektur, in der das mobile Gerät zu einem Firmennetz hinzugefügt wird. Dieser Prozess kann sich in vier Phasen vollziehen. Zunächst wird in Phase 0 eine kryptographisch gesicherte Verbindung etabliert, in der sich der Benutzer authentisiert. Darauf aufbauend kann in Phase 1 die Überprüfung ob die Firmenrichtlinien eingehalten werden durchgeführt werden. Hierzu werden definierte Messwerte erzeugt und mit Hilfe des Policy Decision Point beurteilt, ob sich das Gerät in der gewünschten Konfiguration befindet. Im erfolgreich verifizierten Fall wird der Zugang zum Netz durch den Policy Enforcement Point gestattet (Phase 3).

Falls sich ein Gerät als nicht vertrauenswürdig herausstellt, kann durch ein entsprechendes Quarantänenetz die Möglichkeit eröffnet werden, das Gerät in einen vertrauenswürdigen Stand zu versetzen. Dieses Modell setzt voraus, dass die Kommunikation zwischen dem Benutzer und dem Gerät (Phase 4) als gesichert anzusehen ist.

Ergebnis des Projektes ist eine Sicherheitsplattform, die eine Absicherung mobiler Endgeräte und heterogener mobiler Netze ermöglicht.

Die Plattform soll folgende Funktionalitäten unterstützen:

- zentrale Fernadministration von Netzen mobiler Endgeräte (z. B. sichere Verteilung und entfernte Installation von mobilen Anwendungen auf den Endgeräten, sichere Verteilung von Security Policies auf die Endgeräte und entferntes Unbrauchbarmachen verloren gegangener mobiler Endgeräte),
- Schutz vor Malware (insbesondere Trojanischen Pferden),
- sichere Push-Dienste für mobile Endgeräte,
- Absicherung der Kommunikation zwischen dem mobilen Endgerät und der IT-Infrastruktur des Unternehmens,
- Verschlüsselung von Daten auf den mobilen Endgeräten,
- Firewallschutz für mobile Endgeräte,
- sichere Authentisierung von mobilen Endgeräten gegenüber Servern und dem Backend,
- Herstellerunabhängigkeit (keine Abhängigkeit von bestimmten proprietären Lösungen wie z. B. Nokia Mobile VPN),
- modularer Aufbau, da in verschiedenen Anwendungsszenarien unterschiedliche Sicherheitsmechanismen benötigt werden,
- Bereitstellung geeigneter Administrationswerkzeuge zur Konfiguration der mobilen Sicherheitsplattform unter Berücksichtigung von Usability-Aspekten.

5.1.5 Zwischenfazit

Trusted Computing als Thema von F&E spielt in Deutschland – i. d. R. institutionell eingebettet in breit angelegte Aktivitäten im Bereich IT-Sicherheit – in den letzten Jahren eine zunehmend wichtige Rolle. Zu nennen sind insbesondere die Aktivitäten am Lehrstuhl für Betriebssysteme an der Technische Universität Dresden, am Horst Görtz Institut für Sicherheit in der Informationstechnik, an der Ruhruniversität Bochum, am Institut für Internet-Sicherheit an der Fachhochschule Gelsenkirchen sowie am Fraunhofer-Institut für Sichere Informationstechnologie SIT in Darmstadt.

Begrenzte thematische Schnittstellen sind zudem am Deutschen Zentrum für Künstliche Intelligenz GmbH (DFKI) und dem Transferzentrum für Sichere Software (SiSo) zu finden, die beispielsweise im Auftrag des BSI ein Verifikationstool (Verification Support Environment (VSE-II) zur Spezifikation von Systemkomponenten und Sicherheitszielen entwickelt haben.[49]

An diesen vier respektive fünf Standorten sind - je nach thematischer Abgrenzung - insgesamt etwa 80 bis 150 Wissenschaftler mit TC beschäftigt. Insgesamt lassen sich an Hand der Auswertung der relevanten Quellen sowie der Expertengespräche folgende Einschätzungen aus der Sicht der Scientific-TC-Community festhalten:

- Die noch vor wenigen Jahren anzutreffenden kritischen Einschätzungen zu TC und insbesondere TPM-basierten Lösungen sind inzwischen einer optimistischen Einschätzung und Hervorhebung der positiven Entwicklungsperspektiven durch F&E-Community gewichen. Zwar wird TC immer noch als eine „Janusköpfige“ Technologie bewertet, die sowohl Chancen als auch Risiken birgt, jedoch zeigen die verschiedenen verfolgten Ansätze, dass für die relevanten Probleme und Anforderungen unterschiedliche Lösungsstrategien und -pfade eröffnet worden sind, die durch F&E-Aktivitäten sowohl auf nationaler als auch auf europäischer Ebene prinzipiell als lösbar angesehen werden. Es wird nachhaltig unterstrichen, dass TC eine bedeutende Innovation darstellt, bestehende IT-Sicherheitslösungen zu ergänzen.

- Nach Jahren kritischer Distanz gilt die Arbeit der TCG heute als akzeptiert und bei den meisten als wegweisend, um allgemein anerkannte Standards für Hardware-basierte Sicherheitsfunktionen zu generieren, die gegenüber logischen und physikalischen Angriffen ein hohes Maß an Resistenz aufweisen, deren Implementation und Funktionalitäten nachvollziehbar sind und deren Konformität durch vertrauenswürdige Dritte überprüft werden kann. Die Standardisierungsaktivitäten der TCG werden aktiv oder passiv begleitet, teilweise durch eigene

---

49 Die Hauptanwendungsdomänen dieses Tools bestehen in den Bereichen E-Commerce, E-Payment, E-Government, Pervasive Computing, kryptographische Protokolle, SmartCards, PKI's sowie Signaturgesetz-konforme Komponenten. Vgl. http://www.dfki.de/web/transfer/siso/index_html.

Vorschläge und Einlassungen ergänzt, Zwischenschritte kommentiert oder durch fachlichen Austausch Beiträge zur Optimierung geleistet. Alternative institutionelle Lösungen zur Standardisierung durch die industriellen Akteure sowie die Scientific Community werden als nicht effizient bewertet.

- Während noch vor wenigen Jahren ein weit verbreiteter Optimismus vorherrschte, dass eine Trusted Computing-Architektur eine hinreichend vertrauenswürdige Systemumgebung für alle Betriebssysteme und Arten von Anwendungen bereitstellen würde, gilt inzwischen als allgemein akzeptiert, dass eine „sichere" Hardware und die auf ihr basierenden Funktionalitäten und Prozesse nur dann faktisch den gewünschten Sicherheitszugewinn bereitstellen können, wenn zugleich auch die darauf aufsetzenden Betriebssysteme sicherer gemacht werden. Die nationale, aber auch die internationale Forschung verfolgt mit TC, der Mikrokernel-Strategie sowie der Virtualisierungsstrategie drei sich ergänzende Ansätze, die alle drei einstimmig als Erfolg versprechend bewertet werden. Die Mikrokernel-Strategie sowie die Virtualisierungsstrategie gelten neben TC auch deshalb als wichtig, weil Sie ohne TPM-Funktionalitäten einen Beitrag zur Verbesserung der Systemsicherheit leisten können. Bei beiden Strategien wird Deutschland international zu den führenden Akteuren gerechnet.

- Je mehr die verschiedenen Lösungsansätze Anzeichen der Marktreife erkennen lassen, um so deutlicher hat sich in den letzten Jahren der industriepolitische und standortrelevante Charakter von TC offenbart: TC scheint wesentlich mehr zu sein als eine wichtige, aber begrenzte Facette der IT-Sicherheit, sondern stellt ganz offenkundig eine Schlüsseltechnologie dar, die mit der branchenübergreifenden Migration von Rechenleistung in viele Maschinen, Produkte und Endgeräte des alltäglichen Gebrauchs sowie der immer umfassenderen Vernetzung („Internet der Dinge") beinahe ubiquitäre Verbreitung finden wird. Der Begriff „Schlüsseltechnologie wird insbesondere im Zusammenhang mit „Embedded Systems" verwendet. Vor diesem Hintergrund wird der Entwicklung von Migrations- und Anwendungsszenarien von TC eine strategische und industriepolitische Bedeutung zugewiesen. Es wird eingeräumt, dass man hiervon jedoch noch ein großes Stück entfernt ist. Dies gilt auch im internationalen Vergleich.

- Der Beitrag von TC zur Sicherung der Verfügbarkeit, der Verlässlichkeit, der Vertraulichkeit bei der Generierung, der Speicherung und des Austauschs von Daten kann vor diesem Hintergrund kaum überschätzt werden, allerdings sind noch einige Jahre Entwicklung erforderlich. Angesichts der Tatsache, dass Deutschland ein Industriestandort ist, der nicht nur in den Bereichen Anlagenbau, Maschinenbau, Fahrzeugbau international führend ist und der sich durch die breite Anwendung von Telekommunikations- und Mobilfunkdiensten zu einem der führenden Standorte für Dienstleistungen entwickelt hat, ist der Weiterentwicklung und der raschen Umsetzung der technischen Möglichkeiten von TC

und den darauf basierenden Embedded Systems große wirtschaftliche Bedeutung beizumessen.[50]

- Die volkswirtschaftliche Bedeutung von TC wird unterstrichen dadurch, dass durch TC nicht nur bestehende Aktivitäten z. B. im Bereich Mobile Business Solutions (Remote Access, M-Banking, M-Commerce) sicherer gemacht, sondern dass auch bestehenden Wertschöpfungsketten neue Elemente der Werterzeugung hinzugefügt werden können. Die von einzelnen Akteuren vorgeschlagenen und oben dokumentierten Projektideen machen deutlich, wie viel wirtschaftliches Potenzial sich hinter konkreten Anwendungen etwa im Bereich der Machine-to-Machine-Kommunikation, der vertrauenswürdigen Archivierung, der Übermittlung vertraulicher medizinischer Daten, einem Enterprise Rights Management oder der systemischen Vernetzung von Infrastruktursystemen wie etwa dem Energiebereich verbirgt.[51] TC eröffnet daher große Spielräume für die Generierung von neuen Geschäftsmodellen, indem durch Trusted Systems die notwendigen Enabler-Funktionen zur Verfügung gestellt werden können. Der hierdurch realisierte Zugewinn an Sicherheit könnte durch die Kreierung eines eigenen Labels wie z. B. „IT-Security made in Germany“ vermarktet werden.

- Allen Akteuren ist die industriepolitische Bedeutung von TC bewusst und sie suchen daher den engen Austausch und die Kooperation mit Industrieunternehmen. Der Anwendungsbezug von TC wird unterstrichen durch die Tatsache, dass durch entsprechende Aus- bzw. Neugründungen wie z. B. die Sirrix AG der Technologietransfer in die übrigen Wirtschaftsbranchen erleichtert werden soll. Dieser Transfer befindet sich derzeit noch in den Anfängen. Um die Entwicklung von TC voranzubringen wird ein verstärkter Austausch zwischen den Hochschulen und den industriellen Anwendern für zwingend erforderlich gehalten.

- Nach allgemeiner Einschätzung der im Rahmen dieser Studie befragten Experten wird Deutschland im internationalen Vergleich zu den führenden Akteuren im Bereich TC gerechnet. Ein ähnliches Interesse bzw. vergleichbar vorangeschritten werden entsprechende Aktivitäten in den OECD-Staaten USA[52], dem Vereinigten Königreich[53], Italien[54] und Japan[55] bewertet.

---

50 Vgl. z. B. die von der Internazional School of IT Security (itsis) veranstalteten Workshops zu „Embedded Security in Cars“; http://www.escar.info/.
51 Vgl. Büllingen 2007, S. 6ff.
52 Z. B. University of California; Dartmouth College; http://www.cs.dartmouth.edu/TR2007-594/.
53 Z. B. University of Cambrige.
54 Z. B. Institute of High Performance Computing and Networking (ICAR - Istituto di Calcolo e Reti ad Alte Prestazioni); http://kms.icar.cnr.it/.
55 Z. B. Chuo University of Tokio, Tokai University, IBM Research Laboratory.

- China, aber auch Australien[56] (National ICT Australia (NICTA) mit Fokus auf L4) und Neuseeland[57] werden als Länder eingeschätzt, die mit hohem Tempo Anschluss an die Vorreiterländer suchen. Dabei wird eine regionale TC-Allianz z. B. für den asiatischen Raum unter Einschluss von Japan nicht ausgeschlossen. Insgesamt zeigt sich das wechselseitige Interesse u. a. auch am regen Austausch auf der Ebene des akademischen Nachwuchses oder im Besuch internationaler Konferenzen.

- Dem internationalen Austausch und der grenzüberschreitenden Kooperation wird bei allen Einrichtungen eine hohe Bedeutung beigemessen und dementsprechend durch (internationale) Veranstaltungen, Workshops sowie grenzüberschreitende Projekte Rechnung getragen. Der Grad der Vernetzung im internationalen Kontext wird dementsprechend von allen Gesprächspartnern als sehr hoch bewertet.

- Auf Grund der vergleichsweise geringen Zahl von Akteuren der TC-Community (F&E-Bereich) in Deutschland befinden sich praktisch alle Akteure durch ihre Publikationen, Konferenzbesuche oder gemeinsame Projektarbeit im engen fachlichen Austausch. Die Erfordernisse oder Notwendigkeiten einer Vernetzung werden vor allem auf Grund des Wettbewerbs der Akteure untereinander – abgesehen von der Zusammenarbeit in Großprojekten (EMSCB, Open TC) - eher zurückhaltend bewertet, da die Kooperation in den letzten Jahren nicht immer reibungslos verlief.

- Bei der Förderung entsprechender F&E-Aktivitäten wird Projekten wie Open TC eine wichtige Rolle zugemessen, um die Entwicklung von marktreifen Anwendungen zu beschleunigen. In den Expertengesprächen wurde daher mehrfach die wichtige Vorreiterolle des BMWi, aber auch der EU in den letzten Jahren und die Bedeutung seiner Projektförderung für den hohen und vorangeschrittenen Entwicklungsstand bei TC in Deutschland unterstrichen. Gleichzeitig wurde darauf verwiesen, dass der F&E-Bedarf im vorwettbewerblichen Bereich insbesondere in Hinblick auf den Technologietransfer und die Umsetzung in konkrete Anwendungen als noch erheblich eingeschätzt wird. Dementsprechend sind alle Akteure in hohem Maße an der Förderung neuer Projektideen durch die Bundesregierung interessiert. Von Seiten der Industrie wird jedoch betont, dass eine

---

56 Z. B. The University of New South Wales (UNSW). An der UNSW lehrt heute Prof. Dr. Gernot Heiser (ehem. Karlsruhe), der die Entwicklungstrategie zur Virtualisierung und Miniaturisierung von Betriebssystemen maßgeblich angestoßen hat. Prof Heiser ist Leader des ERTOS-Programms, das für das "Embedded, Real-Time and Operating Systems Programm" steht und beim National ICT Australia (NICTA) angesiedelt ist. Er ist außerdem Gründer und CTO des Open Kernel Labs (OKL), das als eines der führenden Institute im Bereich hoch leistungsfähiger geschützter Betriebssysteme sowie der Virtualisierungstechnologie für Embedded Systems gilt. Vgl. http://www.cse.unsw.edu.au/~gernot/.

57 Vgl. State Services Commission: Trusted Computing and Digital Rights Management Principles & Policies, 2006; www.e.govt.nz.

derartige Förderung nur durch eine enge Zusammenarbeit mit industriellen Anwendern zum Erfolg führen kann.

- Als besondere Unterstützungsmaßnahme für die Aktivitäten wird die Beauftragung von Forschungsprojekten hervorgehoben, deren Dauer und Umfang es erlaubt, z. B. auch aufwändigere Prüf- und Programmierarbeiten durchführen zu können. Es wird darauf hingewiesen, dass der hohe Bürokratieaufwand für die Antragstellung von Forschungsmitteln in erheblichem Umfang Forschungskapazitäten bindet und dass die konkreten F&E-Arbeiten zu TC hierdurch behindert werden.

- In diesem Zusammenhang wird besonders hervorgehoben, dass mit einer breiten Förderung Open Source-basierter Technologien wie z. B. L4 ein Know-how-Vorteil des Standorts Deutschland gesichert werden kann und sollte. Förderprojekte sollten sich einerseits auf die Plattform bzw. die Betriebssysteme beziehen, aber auch wesentlich auf die Entwicklung von Anwendungsszenarien.

5.2 Trusted Computing in der Perspektive der Industrie

5.2.1 Trusted Computing aus der Sicht der Industrieverbände

TeleTrusT Deutschland e. V.

Der in Deutschland maßgebliche fachliche Zusammenschluss von Akteuren für den Bereich Trusted Computing ist der Verein zur Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik TeleTrusT Deutschland e. V. mit Sitz in Berlin.[58]

TeleTrusT sieht es als eine seiner wesentlichen Aufgaben an, unter seinen Mitgliedern für ein gemeinsames Grundverständnis für die TC-Technologie zu werben sowie mögliche Anwendungsfelder und deren Relevanz aufzuzeigen. Hierzu führt der Verein im Rahmen seiner Arbeitsgruppe 2: „Personal Security Environment – PSE“ Diskussionsforen oder Workshops[59] durch und versucht, etwa durch Grundsatz- und Arbeitspapiere[60] die Awareness für TC sowie potenzielle Anwendungen bei den Branchenunternehmen zu erhöhen.

---

58 Vgl. http://www.TeleTrusT.de/.
59 Vgl. z. B.: TC-Workshop 2007 der TeleTrusT-AG „Personal Security Environment – PSE“ am 3.05.2007 an der FH Gelsenkirchen, Institut für Internet-Sicherheit.
60 Vgl. Reimer, Linnemann, Hartmann 30.3.2007, Trusted Computing Whitepaper.

Darüber hinaus sieht sich TeleTrusT als Institution für Sicherheitsfragen in der Rolle, das Know-how der IT-Sicherheitsbranche in die Wirtschaft hinein zu tragen und dort die Awareness auch beispielsweise für die Anforderungen der Interoperabilität zu stärken, wie dies u. a. im Rahmen der Initiative zu „Mailtrust“ (ISIS-MTT) bereits erfolgreich durchgeführt wurde. TeleTrusT signalisiert vor diesem Hintergrund im Rahmen eines für diese Studie geführten Interviews die Bereitschaft, bei der Vernetzung der nationalen TC-Community eine Moderatorenrolle zu übernehmen.

Allerdings thematisiert TeleTrusT auch die weiteren Zusammenhänge wie z. B. die potenziellen Marktbarrieren und weist darauf hin, dass manche Einsatz- bzw. Anwendungsbereiche datenschutzrechtlich relevant sein können, etwa wenn in TPMs gespeicherte Daten hinreichend personenbezogen sind und damit einzelnen Nutzern gezielt zugeordnet werden können. Ferner wird nicht ausgeschlossen, bestimmte Nutzungsoptionen von Betriebssystemen oder Anwendungen an bestimmte Systemzustände zu binden, so dass theoretisch eine Diskriminierung bestimmter Hersteller möglich wird.[61]

Generell allerdings wird unterstrichen, dass die Chancen von TC die potenziellen Risiken deutlich überwiegen. Das Datenschutzrecht, das allgemeine Wettbewerbsrecht sowie das Kartellrecht werden für ausreichend gehalten, um negativen Folgeerscheinungen auch ex-post entgegen wirken zu können. Vor allem aber wird eine frühzeitige Informationspolitik als geeignet erachtet, um gesellschaftspolitische Implikationen zu thematisieren und hierdurch frühzeitig die Weichen für politische Korrekturmaßnahmen zu stellen.

Großer F&E- sowie Gestaltungsbedarf wird derzeit in Hinblick auf die Standardisierung von Datenformaten sowie bei Services und Infrastrukturkomponenten gesehen, um Vertrauensbeziehungen zwischen unbekannten Systemen zu ermöglichen und um diese kostengünstig zu realisieren sowie mit geringem Aufwand zu administrieren. TeleTrusT weist darauf hin, dass es beim gegenwärtig erreichten Entwicklungsstand erforderlich ist, Erfahrungen mit der Errichtung entsprechender Infrastrukturen zu sammeln und weitere Anwendungsgebiete zu erschließen.[62]

Als besonders wichtig wird in diesen Bereichen die Gewährleistung der Interoperabilität angesehen und darauf verwiesen, dass die Entwicklung entsprechender ISO-Standards für die Marktentwicklung unverzichtbar ist. Die Entwicklung und Durchsetzung von ISO-Standards verlangen jedoch viel Zeit und konsensual verlaufende Aushandlungsprozesse. Würde durch nationale Alleingänge im Bereich TC die erforderliche Interoperabilität von Konzepten unterlaufen, so fehlte damit eine der grundlegendsten Voraussetzungen für eine weltweite Durchsetzung. In Zeiten der Globalisierung aber sind Partial- bzw. nationale Lösungen obsolet.

---

61 Vgl. ebd. S. 3f.
62 Vgl. ebd.

Besondere Relevanz für industrielle Anwendungen sieht TeleTrusT z. B. in GRID-Computing, Peer-to-Peer-Kommunikation, Web-Services oder Enterprise Rights Management (ERM). In diesen Anwendungsfeldern besitzt die Sicherung von Vertrauensräumen eine besonders hohe Relevanz zur Bewahrung und Verbesserung von Akzeptanz. In der Förderung entsprechender Initialprojekte wird die Möglichkeit gesehen, dass Deutschland seine Spitzenposition im Bereich TC halten kann und der Transfer von der Forschung und Entwicklung hin zur industriellen Anwendung beschleunigt wird. Als weitere wesentliche Schwerpunkte für entsprechende Pilotierungen werden insbesondere das Online-Banking sowie E-Government-Anwendungen („Bürgerportale“) angesehen.

Andere Industrieverbände

Für die übrigen Verbände der deutschen Wirtschaft wie dem BDI, BITKOM oder DIHT spielt TC - unter Verweis auf die Aktivitäten von TeleTrusT - bislang eine nur eine sehr untergeordnete Rolle. Einschlägige Arbeitsgruppen oder sonstige Aktivitäten sind dort derzeit nicht vorgesehen bzw. erkennbar. Der Branchenverband BITKOM hat das Thema Trusted Computing für 2008 auf seine Agenda gesetzt.

5.2.2 Trusted Computing in der Sicht der Industrieunternehmen

Anbieter von IT-Sicherheitslösungen und Anwendungen

Besonders aktiv im Bereich TC sind naturgemäß diejenigen in- und ausländischen Unternehmen in Deutschland, deren Geschäftsmodell die Herstellung und das Vermarkten von ITK-basierten Anwendungen und IT-Sicherheitslösungen umfasst. Zu nennen sind hier insbesondere Unternehmen wie z. B. Giesecke & Devrient, IBM, Hewlett & Packard, die Infineon Technologies AG, die Siemens IT Solutions and Services AG, Microsoft, SAP AG, die Utimaco Safeware AG, die SECUDE IT Security GmbH, die Sirrix AG Security Technologies oder die SuSE Linux AG. Darüber hinaus ist zu vermuten, dass es innerhalb der heute breit entwickelten IT-Sicherheitsdienstleister-Landschaft in Deutschland zahlreiche Unternehmen gibt[63], die an diesen Aktivitäten indirekt mitwirken bzw. diese aufmerksam verfolgen.[64]

Wie im ersten Teil von Kapitel 4 deutlich wurde, arbeiten fast alle Forschungseinrichtungen in Deutschland im Rahmen von Industriekooperationen z. B. mit Unternehmen wie AMD Saxony Manufacturing GmbH, Daimler Chrysler AG, Infineon Technologies Dresden GmbH & Co. OHG, intel USA, Robert Bosch GmbH, sd&m AG oder net-Linux

---

63 Vgl. z. B. die Aktivitäten der Sysgo AG; http://www.sysgo.com/.

64 Die Zahl der in Deutschland aktiven IT-Sicherheitsdienstleister wird auf mehrere tausend geschätzt. Einstellung und Awareness zu TC können daher nur im Rahmen einer gesonderten Markterhebung analysiert werden.

im Bereich TC zusammen. Dies bedeutet, dass hier auf Seiten verschiedener Vorreiterunternehmen wie z. B. der deutschen Automobilindustrie ein eigenes Interesse vorherrscht, in die Suche nach bzw. in die Entwicklung von TC-Lösungen zu investieren. Die im Rahmen dieser Studie befragten Experten weisen darauf hin, dass dieses Engagement noch wesentlich vertieft werden könnte und auf eine deutlich breitere industrielle Basis gestellt werden sollte, um die vorhandenen Potenziale ausschöpfen zu können.

Bei den im Rahmen dieser Studie befragten Unternehmen wurde darauf hin gewiesen, dass Deutschland in einer international führenden Rolle im Bereich TC gesehen wird und dass durch die Mitarbeit in der TCG der fachliche Austausch und die Teilhabe am internationalen Standardisierungsprozess realisiert wird. Befürchtungen, dass hierbei Know-how deutscher Akteure abfließt und dieses auch den marktmächtigen wettbewerblichen Playern zu Gute kommt, wird mit dem Argument begegnet, dass in der TCG i. d. R. nur solches Wissen verhandelt wird, das durch Patente bereits geschützt ist. Zu dieser Sichtweise passt auch das Vorhaben der TCG, ihre Standards zu ISO-Standards zu migrieren. Insofern dient die Arbeit in der TCG stets auch dazu, die Verbreitungs- und Vermarktungschancen für eigene Ansätze auf eine breitere Basis zu stellen.

Es wird unterstrichen, dass für die wesentlichen grundlegenden Problem- und Anwendungsfelder im Rahmen von EMSCB/TURAYA Demonstratoren geschaffen wurden. Der entscheidende Schritt besteht nun darin, den Know-how- und Technologietransfer in die Industrie zu organisieren. Besonders hohe Erwartungen werden in Bezug auf den Bereich der „Embedded Systems“ geäußert. Unter den Befragten gibt es daher auch kritische Stimmen, die die noch große Anwendungsferne der im Rahmen von EMSCB entwickelten Demonstratoren bemängeln und deren Weiterentwicklung hin zu industriellen Anwendungen für zwingend erforderlich erachten.

Als denkbare Organisationsform für eine Anwendungs-, Umsetzungs- und Förderstrategie wird ein öffentlicher Projektwettbewerb vorgeschlagen, um durch Initialprojekte Erfolg versprechende Anwendungen zu pilotieren. Der Vorteil dieser Lösung wird darin gesehen, dass die Industrie im Rahmen eines Förderwettbewerbs selbst initiativ werden kann und muss, wenn entsprechende Lösungen gefördert werden sollen. Allerdings könnte auch die Fraunhofer-Gesellschaft (SIT) eine koordinierende und aktivierende Rolle beim Technologie-Transfer übernehmen.

(Potenzielle) Anwender von TC-Lösungen

In einzelnen Anwendungsbranchen wie z. B. dem Automobilbau sind die Erwartungen an TC hoch und werden dort seit einigen Jahren mit gewisser Energie verfolgt.[65] In der Sicht einiger Experten gilt der Automobilbereich sogar als der Bereich, der beim Einsatz von Embedded Systems am weitesten fortgeschritten zu sein scheint. Im Fokus stehen

65 Vgl. Z. B. Weimerskirchen et. al. o. J. sowie Wollinger 2007.

hierbei solche Verfahren, die vor vorsätzlicher Manipulation schützen oder der Schutz digitaler Rechte etwa in Zusammenhang mit der Nutzung von Medien in Automobilen. Als Vorreiter gelten hier etwa die Firmen Blaupunkt sowie Bosch. Solche Vorkehrungen sind beispielsweise beim Digitalen Tachografen, beim Schutz vor gefälschten Elektronikbauteilen, beim Diebstahlschutz oder beim Bezahlen digitaler Inhalte von hoher Bedeutung.

Darüber hinaus werden auch Anwendungen z. B. in der Car-to-Car Kommunikation, beim Traffic Management oder bei der Elektronischen Maut verfolgt und entwickelt. Als entscheidend wird hierbei ein Systementwurf betrachtet, der die unterschiedlichen Sicherheitsfacetten integriert. Im Ergebnis wird eine Flut von neuen Geschäftsmodellen erwartet, die IT-Sicherheit zu einem zentralen Anwendungsfeld in zukünftigen Automobilgenerationen macht.[66] Vor diesem Hintergrund finden Veranstaltungen wie z. B. die Veranstaltung escar (Embedded Security in Cars) statt, um über den Entwicklungsstand, die technischen Herausforderungen sowie die verfolgten Lösungsansätze zu kommunizieren.[67]

Für den Bereich der Investitionsgüter, des Maschinen- und Anlagenbaus oder der Versorgungsbereiche (Energie, Gas, Wasser) werden ebenfalls als große Einsatzfelder für IT-Sicherheit im Allgemeinen und TC-Lösungen im Besonderen angesehen, wenn es etwa darum geht, Schaltelemente, Sensoren oder Smart Meter zu sichern und gegen Manipulation zu härten. Die Entwicklung von Einsatzszenarien und die Förderung entsprechender Pilotprojekte werden als wichtige vorbereitende Schritte für eine Markterschließung angesehen. Generell werden alle Einsatzgebiete für TC als interessant betrachtet, bei der die verwendete Hard- und Software während des Lebenszyklus nicht oder nur wenig verändert wird.

Als eine weitere interessante Applikation wird das Zusammenspiel zwischen dem Einsatz von TPMs als vertrauenswürdigen Sicherheitsanker in einer gegebenen Plattform und dem Einsatz von Smart Cards betrachtet. Prinzipiell genügen Smart Cards allerhöchsten Sicherheitsanforderungen (CC EAL 4 SOF-hoch) und ermöglichen die Speicherung und Nutzung von personalisierten Daten, Programmen und Onlinedienstleistungen. So kann mit Hilfe einer Smart Card z. B. der Zugang zu einer Plattform autorisiert und der Zugriff auf Daten flexibler gestaltet werden. Auf diese Weise würden Migrationsprobleme z. B. bei nomadischer Nutzung deutlich reduziert, da die erforderlichen Daten auf der Smart Card gespeichert und dort verbleiben würden[68]. Auch könnte mit Hilfe einer Smart Card eine qualifizierte digitale Signatur geleistet werden. Eine wesentliche Voraussetzung für eine kompatible Nutzung von Smart Card und TPM wäre die Schaffung eines vertrauenswürdigen Kanals.[69]

---

66 Vgl. Lemke et al. 2006.
67 Vgl. http://www.escar.info/07/general.html.
68 Abweichend hierzu Stumpf / Sacher / Roßnagel / Eckert, 2007, S. 359f.
69 Vgl. Gawlas / Meister 2005, S. 517ff.

Technische Überlegungen, die Smart Card als mobiles TPM zu nutzen, werden in den Expertengesprächen sehr skeptisch beurteilt, weil der Sicherheitsgewinn, der durch eine feste Verlötung eines TPMs auf einer Plattform gewonnen wird, durch eine solche Lösung ohne Not verspielt würde.

Andere Branchen wie z. B. die Telekommunkationsanbieter hegen in Bezug auf Herstellung und Überprüfbarkeit von „Reputation“ in den Netzen große Erwartungen, da dies für alle Netz-basierten Geschäftsmodelle von essentieller Bedeutung ist. Die gilt insbesondere für Machine-to-Machine-Anwendungen. Generell wird die Generierung von „Vertrauen“ in offenen TK-Netzen als eine der größten aktuellen und künftigen Herausforderungen angesehen. Dabei werden in diesem Zusammenhang eine Reihe von offenen Fragen, Schwierigkeiten und potenziellen Markthürden thematisiert:

- auf Grund der globalen Netzwerkarchitektur sind Standardisierungsprozesse auf internationaler Ebene (ISO) erforderlich, um die Interoperabilität zu gewährleisten. Der Zeitaufwand wird als erheblich eingeschätzt.

- es existiert für Lösungen im Netz stets eine kritische Masse, die erst erreicht werden muss, um ein „Umschalten“ in eine Massenanwendung zu ermöglichen. Es wird daher thematisiert, durch welche (Killer-) Applikationen diese kritische Masse erreicht werden kann.

- ein Ansatzpunkt für die Verbreitung von TC-Lösungen wird darin gesehen, wenn es gelänge, ökonomische Anreize für deren Verwendung zu setzen beispielsweise bei Banken oder Versicherungen.

- ein Mehr an Sicherheit für neue Geschäftsmodelle z. B. in den Bereichen Mobile Banking oder Mobile E-Health ist wünschenswert, wird aber in Hinblick auf die staatlichen Sicherheitsanforderungen (Vorratsdatenspeicherung, „Bundestrojaner“) als „schwer“ kommunizierbar betrachtet.

- es wird auf die Vielzahl alternativer Sicherheitslösungen wie z. B. VPN, Firewalls, Sicherheits-Suiten, Festplattenverschlüsselung etc. hingewiesen, deren Nutzung bereits weitgehend eingeschwungen ist, die am Markt verbreitet sind und bei deren Einsatz wirtschaftliche Vorteile vermutet werden. So werden nach einer Leserumfrage der IT-Sicherheitszeitschrift kes durch die Besitzer mobiler Endgeräte in 98% aller Fälle Virenscanner, bei 83% eine Personal Firewall und bei 40% eine Dateiverschlüsselung eingesetzt.[70]

- vor diesem Hintergrund wird der Nutzen von TC-basierten Lösungen z. B. in mobilen Geräten hinterfragt. Entsprechend der oben zitierten kes-Umfrage setzen lediglich 4% die Funktionalitäten eines TPM ein, obwohl dies heute in fast

70 Vgl. kes Leserumfrage Mai 2007.

allen mobilen Geräten implementiert ist und die entsprechenden Funktionalitäten durch eine entsprechende Software aktiviert werden können.[71] Die vergleichweise geringe Nutzung des TPM wird von Experten u. a. mit der geringen Nutzerfreundlichkeit der Tools begründet.[72]

- es wird darauf hingewiesen, dass der Einsatz von TC in Betrieben komplexe Managementlösungen erfordert um z. B. Anwendungen wie Enterprise Rights Management umzusetzen. Hierbei darf jedoch kein höherer Administrationsaufwand entstehen.

- es werden Befürchtungen geäußert, dass TC-basierte Sicherheitslösungen zu (heute noch nicht näher spezifizierbaren) Kosten führen, die vom Nutzer nicht oder nur widerwillig akzeptiert werden.

Insgesamt wird hervorgehoben, dass der Nutzen von TC-Lösungen erst einmal demonstriert und seine Vorteile unter Beweis gestellt werden müssen. Die Awareness in der Industrie hierfür wird – mit Ausnahme einzelner Unternehmen etwa aus dem Bereich der Automobilzulieferer - aus heutiger Sicht bislang als eher gering angesehen, entsprechend der von einem der befragten Experten formulierten Sentenz: „die Unternehmen, aber auch die normalen Nutzer, haben sich doch längst an den Bedrohungszustand im Netz gewöhnt. Sie haben in Lösungen investiert und die funktionieren weitgehend. Verluste gibt es überall und immer und wir werden lernen, damit zu leben“.[73]

Als eines der wichtigsten Felder bei TC-Lösungen wird das DRM angesehen. Es wird betont, dass die mit diesem nach wie vor hoch sensiblen Thema verbundenen Fragen nur dann allseitig befriedigend gelöst werden können, wenn von Seiten der Politik eindeutige Rahmenbedingungen vorgegeben werden, die es den Akteuren der Branche ermöglichen, hierauf befriedigende und nachhaltige Antworten bzw. entsprechende Geschäftsmodelle zu entwickeln. Der Staat sollte sich an der Entwicklung entsprechender Einsatzszenarien beteiligen und den Prozess zwischen allen Akteuren moderieren. Hierdurch würde die Möglichkeit eröffnet, neben den Anbietern auch die relevanten Anwendergruppen frühzeitig einzubinden, um deren Akzeptanz zu sichern.

---

71 Vgl. z. B. die sog. HPProtectTools, die sechs verschiedene Sicherheitsmodule umfassen und die die Firma Hewlett & Packard auf den von ihr vermarkteten Notebooks installiert: www.hp.com/products/security. Vgl. dazu ferner die Software-Produkte der Firma SafeBoot: http://www.safeboot.com/products/device-encryption/.

72 Vgl. z. B. Vorträge auf dem „Secure Mobile Computing“ KompetenzTag des TelekomForum am 17. Oktober 2007.

73 Anonymes Zitat aus einem im Rahmen dieser Analyse durchgeführten Interview.

5.2.3 Zwischenfazit

- In der Perspektive der Wirtschaft und der Verbände gilt Deutschland als eines der im Bereich IT-Sicherheit (Hochsicherheitslösungen) sowie bei TC führenden Länder. Es wird betont, dass Deutschland die wissensmäßigen Voraussetzungen besitzt, diese Spitzenposition zu halten oder sogar auszubauen, wenn die bestehenden Lösungsansätze weiter verfolgt werden. TC wird – mit Blick auf Embedded Systems - hierbei einstimmig das Potenzial einer Basisinnovation zuerkannt. Es werden allerdings Schwierigkeiten und Hürden gesehen, entsprechende Lösungen marktfähig zu machen. Hierbei wird auf die längere Zeitspanne verwiesen, die erforderlich ist, bevor TC-Lösungen den Massenmarkt erreichen. Es sollen daher Felder identifiziert werden, von denen eine Initialzündung ausgehen könnte und die den tatsächlichen Nutzen demonstrieren können.

- Wichtige industrielle Akteure, die Forschung sowie das BSI sind in die Standardisierungsaktivitäten der TCG involviert und haben damit Einfluss auf die internationale Entwicklung. Die noch vor wenigen Jahren geäußerte Kritik, das bei der TCG repräsentierte Wissen sei insbesondere für den interessierten Kreis von KMU nur schwer zugänglich, wird von keinem der Interviewpartner geteilt. Es wird vielmehr betont, dass alle relevanten Informationen allen Akteuren zur Verfügung stehen, jedoch – entsprechend der Größe der Unternehmen und der Ausstattung mit Ressourcen – unterschiedlich ausgeprägte Nutzungschancen bestehen. Nach der Senkung der Mitgliedsbeiträge der TCG werden jedenfalls keine finanziellen Barrieren für den Know-how Transfer gesehen.

- Die im Bereich von F&E entwickelten verfolgten Lösungen (EMSCB / TURAYA, Open TC) sind dem mit TC eng befassten Kreis von industriellen Akteuren bekannt. Es besteht der Wunsch, dass diese Entwicklungen aus dem eher noch praxisfernen Demonstratorenstatus in einen anwendungsnäheren Status überführt werden sollten. In diesem Zusammenhang wird die Bedeutung der Arbeiten an der TU Dresden (Mikrokernelentwicklung, Virtualisierung) besonders hervorgehoben und die Notwendigkeit einer Kooperation auf nationaler Ebene unterstrichen.

- Im Bereich der (potenziellen) Anwenderbranchen hingegen nimmt der Aufmerksamkeitsgrad – bis auf wenige Ausnahmen wie z. B. im Automobilbau - beinahe schlagartig ab. Hier ist ein grundlegendes Awareness-Problem gegenüber den mit TC zu realisierenden Marktchancen zu diagnostizieren. Es wird als richtig und dringend erforderlich angesehen, die Aufmerksamkeit über alle Branchen hinweg durch geeignete Schritte zu erhöhen. Hierbei könnten die Verbände potenziell eine wichtige Transmissionsfunktion übernehmen.

- Wie in vielen anderen Hochtechnologiebereichen wird der Technologietransfer als Engpass und Kernpunkt einer auf die Verbreitung von TC gerichteten industriepolitischen Agenda bezeichnet. Es wird die Entwicklung einer „Roadmap“ zu TC gefordert, die allen Akteuren die Bestimmung ihrer Interessen und ihrer Rollen ermöglicht. Der Branchenverband TeleTrusT hat die Bereitschaft erkennen lassen, alle einschlägigen Vernetzungsaktivitäten zu unterstützen und an der Etablierung einer Industrie-übergreifenden Plattform mitzuwirken.

- Die Förderung von Initialprojekten etwa im Rahmen von gemeinsamen Projekten von öffentlichen Institutionen und der Industrie wird als eine der wichtigsten Möglichkeiten angesehen, den erwünschten Technologietransfer in die industrielle Breite anzustoßen und zu verbessern. Interessante Schwerpunkte für Pilotierungen werden z. B. beim Online-Banking sowie bei E-Government-Anwendungen („Bürgerportale“) gesehen, die auch schon in der Vergangenheit durch Aktivitäten in Deutschland besonders intensiv geprägt wurden.

- Weitere Anwendungsfelder werden überall dort gesehen, wo vertrauliche Daten und Anwendungen gegenüber dem Zugriff Dritter oder gegen Manipulation geschützt werden sollen. Damit verbunden sind oft völlig neue Geschäftsmodelle, die auf einer verbesserten Vertrauenssituation aufbauen können. Solche Anwendungsbereiche werden insbesondere gesehen bei:

    - Car Service Software
    - Car Entertainment
    - Enterprise Rights Management
    - Geräteverschlüsselung
    - Home Office
    - Geldautomaten
    - Supply Chain Management
    - Wahlcomputern
    - Mobilen Endgeräten
    - Firmenkommunikation (Client Server Systeme)
    - eHealth
    - eCommerce

- Webservices
- Grid Computing
- VoIP
- Haustechnik
- Telekommunikativen Vernetzungen der Versorgungsbereiche (z. B. eEnergy, Smart Metering).[74]

- Die Bedeutung von ISO-Standards wird als zentral angesehen, um allen TC-basierten Lösungen insbesondere im Bereich der Telekommunikationsnetze zur Interoperabilität zu verhelfen.
- Als großer Anwendungsbereich im Bereich IT-Sicherheit gilt künftig, Nutzer in die Lage zu versetzen, bewusste Entscheidungen bzgl. der Anwendung von einzelnen Sicherheitstools treffen zu können. Es wird vorgeschlagen, bei einem der Industrieverbände wie z. B. Teletrust eine Task Force ins Leben zu rufen, die die Einsatzmöglichkeiten speziell mit dieser Ausrichtung ausloten soll.

74 Vgl. TURAYA Animationsfilm Textfassung vom 31. August 2007.

6 Die Behandlung von Trusted Computing auf EU-Ebene

Trusted Computing ist auch auf der Ebene der EU seit einigen Jahren ein wichtiger Gegenstand der Befassung. Bedeutendste Projekte in diesem Zusammenhang sind Open Trusted Computing (a) sowie Robust Open Infrastructure (ROBIN) (b). Daneben führt die Kommission im Rahmen von IT-Sicherheitskonferenzen auch TC-bezogene Veranstaltungen bzw. Workshops durch (c).

a) Open Trusted Computing

Seit 2002 wird im Rahmen des 6. Rahmenprogramms für gemeinschaftliche Forschung (FP6 European Community Framework Programme for Research, Technological Development and Demonstration) das Projekt Open Trusted Computing von der EU-Komission co-finanziert. Das Projekt wird koordiniert von der österreichischen Firma Technikon Forschungs- und Planungsgesellschaft mbH.

Open Trusted Computing verfolgt im wesentlichen drei Zielsetzungen:

- Die Entwicklung eines sicheren Betriebssystems,
- Die Entwicklung einer entsprechenden Kontroll-Software in Kombination mit einem sicheren Betriebssystem, sowie
- Die Entwicklung prototypischer Anwendungen.

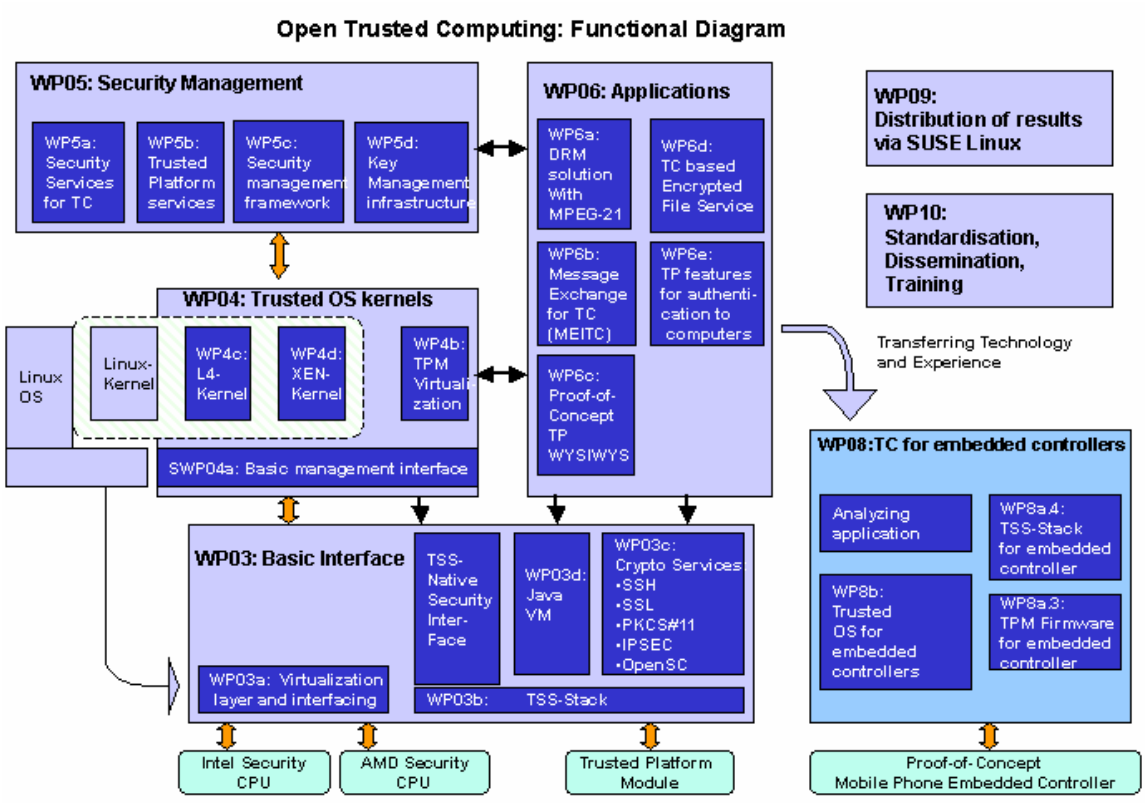
Die mit Open TC verfolgten Zielsetzungen sind sehr ambitioniert: Das Open TC Konsortium verfolgt die Festlegung und Implemenentierung eines Rahmenwerks für Open Trusted Computing. Die Architektur basiert auf Sicherheitsmechanismen, die auf den tieferliegenden Schichten des Betriebssystems abgegrenzte Bereiche mit eigenen Zugriffsrechten sowie Schnittstellen zur Plattform-Hardware zur Verfügung stellen. Diese Schichten ermöglichen die Implementierung von erhöhter Sicherheit und für herkömmliche Betriebssysteme, die Middleware sowie Anwendungen.[75]

In Open TC werden sichere Varianten verschiedener Linux-Versionen als Open Source entwickelt, um diese Technik der sicheren Betriebssysteme auch der Allgemeinheit zur Verfügung stellen zu können. Insgesamt beinhaltet Open TC 10 Arbeitsschwerpunkte, die die verschiedenen Fragestellungen abdecken (vgl. Abbildung 6-1). Folgeprojekte für sichere, offene Betriebssysteme auf Embedded und anderen Prozessorplattformen sind geplant.

---

75 Vgl. www.Open TC.net/index; (Übersetzung aus dem Englischen durch die Autoren).

Abbildung 6-1: Arbeitsschwerpunkte von Open Trusted Computing



Quelle: Open Trusted Computing

Das Projekt, das ingesamt 23 Partner zählt, ist eng vernetzt mit den deutschen TC-Aktivitäten des EMSCB-Projektes. Am Forschungsverbund Open TC sind aus Deutschland die Technische Universität München (TUM), die Technische Universität Dresden, die Ruhruniversität Bochum, infineon Technlogies, SUSE Linux Enterprise sowie das Institut für Technikfolgen-Abschätzung (ITAS) Karlsruhe beteiligt. Daneben sind weitere industrielle sowie akademische Projektpartner aus Italien, Belgien, Bulgarien, Frankreich, Österreich, der Türkei, den USA (AMD, IBM, HP), sowie dem Vereinigten Königreich in Open TC involviert.

Wichtige Ergebnisse werden auf der Web-Site von Open TC veröffentlicht. Für die Projektmitglieder besteht ein geschützter Zugangsbereich.

b) Robust Open Infrastructure (ROBIN)

Im Rahmen des 7. EC RTD Programms, das von 2007 bis 2013 laufen wird und sich in wesentlichen Teilen der IT-Sicherheits-bezogenen Forschung und Entwicklung widmet, werden Aktivitäten zu Absicherung von Rechnerplattformen innerhalb offener Netzwerke gefördert. Das Projekt geht im Wesentlichen auf die Forschung der TU Dresden zurück und baut auf dem Projektstand von VFiasco auf. Die Projektleitung liegt daher in den Händen der TU Dresden (Lehrstuhl Prof. H. Härtig). Von deutscher Seite ist ferner die Firma secunet beteiligt. Hinzu kommen weitere Hochschul- und Industriepartner sowie eine Nutzergruppe aus zwei weiteren EU-Staaten (Universität Nijmwegen, ST-Microelectronics).

Ziel der F&E-Aktivitäten ist die Entwicklung einer offenen (europäischen) Plattform, die sich bewusst als Gegenstück zu den in naher Zukunft zu erwartenden proprietären amerikanischen Lösungen positioniert. Es geht darum, eine Variante der L4/Nizza-Architektur zu implementieren, welche die Möglichkeiten neuer HW-Architekturen nutzt. In diesem Zusammenhang soll eine im Vergleich mit L4VM wesentlich kleinere Trusted Computing Base für Virtualisierungsprozesse entwickelt werden. Auf der Grundlage der theoretischen Informatik sollen Schnittstellen formal spezifiziert und deren Umsetzung in ein Betriebssystem verifiziert werden. Es ist vorgesehen, dass die Partner secunet und ST-Microelectronics Demonstratoren zur Verfügung stellen, mit deren Hilfe später konkrete Produkte entwickelt werden können.

c) IT-Sicherheits-bezogene Arbeitsgruppen und Veranstaltungen

Die Sicherheitsproblematik in offenen Telekommunikationsnetzen sowie alle Aspekte der Generierung von Vertrauen spielen bei der Europäischen Kommission und speziell in der Sektion „Information Society and Media“ eine immer wichtigere Rolle. Dies zeigt sich beispielsweise an der Gründung des SecurIST Advisory Boards sowie der EU Security and Dependability Task Force (STF).[76]

Der SecurIST Advisory Board hat am 15. Januar 2007 die “Empfehlungen für ein Rahmenwerk zur Erforschung von Sicherheit und Zuverlässigkeit: Von der Sicherheit und Zuverlässigkeit durch zentrale Vorgaben zu einer Sicherheit und Zuverlässigkeit durch Kompetenz und Fähigkeit“ veröffentlicht. In diesen Empfehlungen befaßt sich der Advisory Board u. a. auch mit den verschiedenen Optionen bei Sicherheitstechnologien. Zu den Kerntechnologien werden zum einen die Verschlüsselungstools und zum anderen Technologien zur Vertrauensgenerierung gezählt. Im Einzelnen heißt es hierzu: Die Verfügbarkeit vertrauenswürdiger Funktionalitäten umfasst im Kern eine Verallgemeinerung vertrauenswürdiger (…) Hardware, TPMs, Mikrocodes, Kernels, grundlegender Aspekte von Betriebssystemen bis hin zu spezifizierten Programmierschnittstellen: all

76 Bei der STF handelt es sich um eine interdisziplinär zusammengesetzte Runde aus renommierten Vertretern aus Forschung und Lehre sowie Industrieunternehmen.

dies kann genutzt werden, um eine vertrauenswürdige lokale Umgebung zu schaffen. Eine solche Architektur kann dafür sorgen, dass Informationen sicher verwendet werden und nur so wie vom Anwender beabsichtigt. Wie schon an früherer Stelle bemerkt, die Implementierung kryptografischer Prozesse erfordert zwingend eine solche vertrauenswürdige Umgebung.[77]

Der SecurIST Advisory Board führt Workshops durch, deren Ergebnisse in Form des SecurIST Reports veröffentlicht wurden.[78]

Die Gründung der STF zielt nach den Ereignissen vom 9. November 2001 insbesondere auf eine verbesserte Kommunikation zwischen wichtigen Akteuren in Europa und den USA. Vor diesem Hintergrund wurde 2006 eine Plattform für den fachlichen Austausch zwischen europäischen sowie US-amerikanischen Forschungsinstituten und Behörden ins Leben gerufen.

Der 1. EU-US Summit fand vom 15. bis 16. November 2006 in Dublin statt mit dem Titel: Cyber Trust: System Dependability & Security. Insgesamt wurden im Rahmen dieser Tagung sechs Einzelveranstaltungen durchgeführt. Das Thema Trusted Computing wurde hierbei allerdings nur indirekt adressiert z. B. im Rahmen von Forum 6, das sich u. a. mit der Entwicklung und Funktionalität von geeigneten Testmöglichkeiten befaßte.

Der 2. Workshop der EU-US Summit Series on Cyber Trust fand am 26. und 27. April 2007 in Monticello (Illinois) statt zum Thema: ”Secure, Resilient & Trusted ICT Infrastructures in ICT – FP7”.[79]

---

77 Vgl. SecurIST Advisory Board, S. 28. (Die Übersetzung aus dem Englischen erfolgte durch die Autoren).
78 Vgl. z. B. SecurIST Report zum Joint Workshop: Security & Dependability in Mobile and Wireless: Future requirements for R&D, Brussels 11. und 12. Mai 2006.
79 Alle Unterlagen und Papiere stehen zum Download bereit auf der Homepage der ICT Security & Dependability Task Force http://www.securitytaskforce.org/index.

7 Die Behandlung von Trusted Computing in ausgewählten außereuropäischen Ländern

Seit der Debatte um Trusted Computing und der Gründung der TCG sind angesichts der Bedeutung des Themas entsprechende Aktivitäten insbesondere im F&E-Bereich in allen hochindustrialisierten Ländern zu beobachten. Ein Blick auf die in der TCG mitarbeitenden Unternehmen zeigt, dass dort neben den anglo-amerikanischen und europäischen Ländern auch Akteure aus den asiatisch-pazifischen Staaten wie z. B. China, Japan, Australien oder Neuseeland vertreten sind.

7.1 Trusted Computing in China

Fast alle Aktivitäten, die sich in China mit TC befassen, sind im wesentlichen beinflusst durch eine koordinierte zentralstaatliche Einflussnahme. Die entsprechenden politischen Vorstellungen und Vorgaben werden allerdings in enger Zusammenarbeit mit den einschlägigen chinesischen Unternehmen der ITK-Branche sowie den mit TC befassten Forschungseinrichtungen entwickelt.

In der Politik gilt TC als eine Schlüsseltechnologie, um ein eigenes nationales Sicherheitssystem zu etablieren, während chinesische Unternehmen angesichts des intensiven internationalen Wettbewerbs mit immer geringeren Margen sowie der Marktdurchdringungsstrategien ausländischer Konzerne hierin eine Möglichkeit sehen, ihre Marktanteile durch Produktdifferenzierung zu verteidigen. Allerdings werden im Kontext von IT-Sicherheit und TC starke Anstrengungen unternommen, oppositionelle gesellschaftliche Gruppen zu überwachen bzw. zu kontrollieren.

Angesichts der unterschiedlichen Interessenlagen gibt es Anzeichen dafür, dass innerhalb der Branchenunternehmen in den letzten Jahren eine kontinuierliche Diskussion über TC stattfindet, während die breite Öffentlichkeit in diese Debatte bislang allenfalls marginal involviert ist.

7.1.1 Entwicklung in der Vergangenheit

Die Ursachen der Beschäftigung mit TC in China gehen zurück bis in die Zeit, als im Zuge des Zusammenbruchs der sozialistischen Länder Osteuropas zunehmend Sicherheitsbedenken die Diskussion über Sicherheit der Telekommunikationsinfrastruktur zu bestimmen begannen. So wurde 1994 eine Verordnung zur Aufrechterhaltung der Computer- und Informationssicherheit (Ordinance of Computer Information Security) erlassen, die seither das allgemeine rechtliche Rahmenwerk für entsprechende nationale Maßnahmen bildet. Mit der allmählichen Verbreitung der Internetnutzung wurde die-

ses Rahmenwerk wiederholt angepasst und durch weitere Gesetze zur Sicherung kritischer Infrastrukturen ergänzt.[80]

Erst Ende der 90iger Jahre wurde IT-Sicherheit bzw. Trusted Computing erstmals zu einem Thema einer breiteren öffentlichen Diskussion, als der amerikanische Chip-Hersteller Intel mit der Markteinführung des Pentium III im Jahr 1999 eine CPU-ID einführte, deren technische Spezifikationen eine Verifikation der jeweiligen Chip-Identität und der entsprechenden Hardwareumgebung über das Internet möglich machte. Als unmittelbare Reaktion auf diese Entwicklung wurden alle PCs in der Administration von Regierung und Militär physisch vom Internet getrennt. In Hinblick auf die Beschaffung von weiterer Hardware für öffentliche Stellen wurden in den Jahren darauf Intel sowie insbesondere Microsoft von verschiedenen Vergabeverfahren im Umfang von mehreren Milliarden Dollar ausgeschlossen.

Durch den mit diesem Vorkommnis verbundenen Schock begann sich in der chinesischen Politik die Erkenntnis durchzusetzen, dass nationale Sicherheitsinteressen nur auf der Basis vertrauenswürdiger Technologien und Produkte abgesichert werden konnten. Vor diesem Hintergrund wurden eine Reihe verschiedener F&E-Projekte angestoßen, um auf einer möglichst breiten technologischen Basis alle Schlüsselelemente vom BIOS, über Chips und Platinen bis hin zu Netz- und Servertechnologien sowie Betriebssysteme in nationaler Eigenregie herstellen zu können. Durch entsprechende Verordnungen wurde in diesem Prozess sichergestellt, dass ein Teil der F&E-Aktivitäten sowie die Herstellung und Vermarktung bestimmter Schlüsselkomponenten enger staatlicher Kontrolle unterlagen.

Vor diesem Hintergrund wurden die TC-Aktivitäten in den westlichen Industriestaaten und die Gründung der TCG mit großer Aufmerksamkeit verfolgt. Mit staatlicher Zustimmung arbeiten Vertreter der beiden großen Computerfirmen Lenovo - drittgrößter PC-Hersteller der Welt - sowie das auf Sicherheitslösungen spezialisierte Unternehmen Sinosun seit einigen Jahren in der TCG mit. Der Vertreter von Lenovo, derzeit Randy Springfield, ist im TCG Board of Directors vertreten. Sinosun gehört zum Kreis der TCG-Adopter und produziert seit 2005 ein mit dem TCG-Standard V 1.2 konformes TPM.

Parallel zu den internationalen Aktivitäten in der TCG wurde 2005 die sog. „Chinese Trusted Computing Group" (CTCG) ins Leben gerufen, die insgesamt etwa 120 Mitglieder sowohl aus den öffentlichen Institutionen und dem Hochschulbereich als auch aus

---

80 Dieses Rahmenwerk umfasst u. a. Maßnahmen zur "Security Protection Administration of the International Networking of Computer Information Networks" (MPS 1997), Maßnahmen für die "Administration of Internet Information Services" (2000), Maßnahmen für die "Prevention and Control of Computer Virus" (MPS 2000), den "Electronic Signature Act" (2004), "Administrative Measures on the Ciphers in Electronic Authentication" (OSCCA, 2005) sowie Maßnahmen für die "Administration of the Maintenance of Secrets in the International Networking of Computer Information Systems Provisions" (OSCCA, 2005).

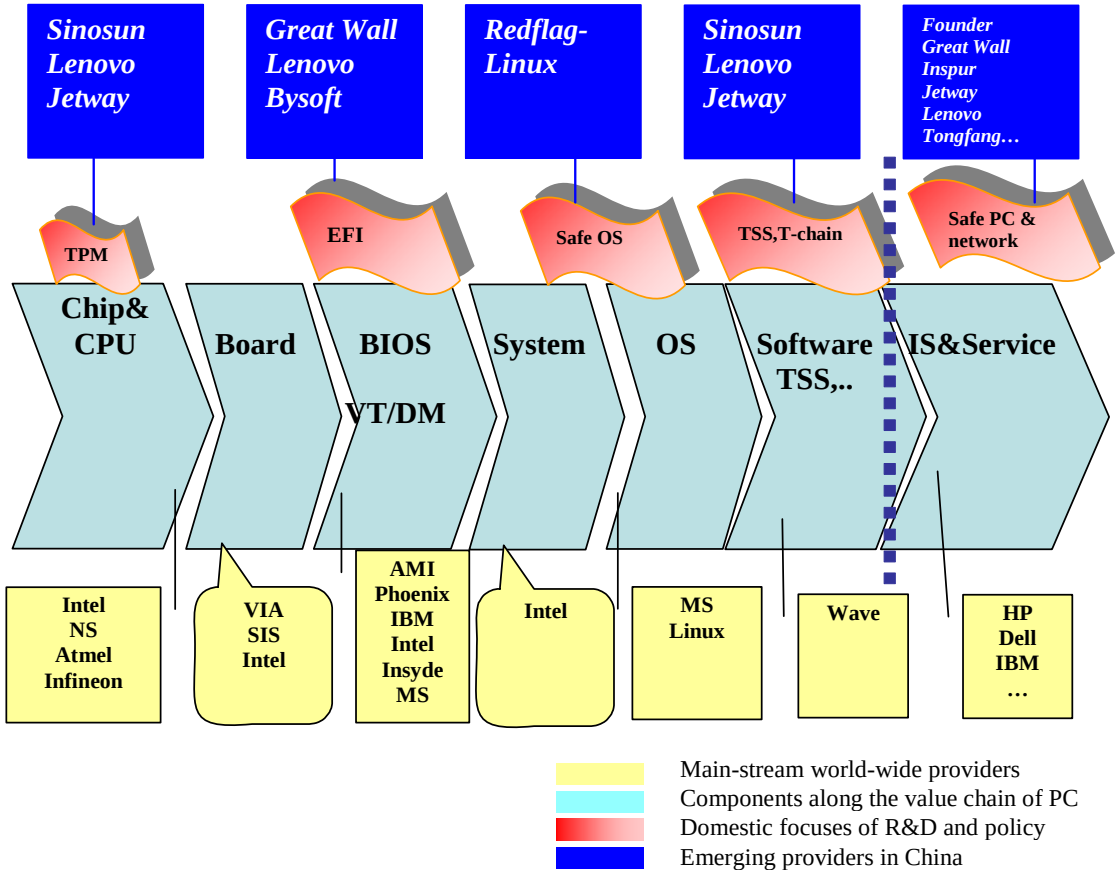
der Wirtschaft umfasst. Die Aktivitäten der CTCG wurden verstärkt, als Mitte 2006 bekannt wurde, dass einige große amerikanische Herstellerfirmen Hardwareprodukte mit nicht-zertifizierten TPMs an ihre Kunden vermarkteten. Vorkommnisse wie diese bestärken die chinesische Regierung, dass die nationale Sicherheit ausschließlich auf der Basis eigenständiger nationaler Entwicklungen basieren sollte. Um dieser Einschätzung Geltung zu verschaffen, wurde nur wenige Monaten später durch ein Gesetz verbindlich vorgeschrieben, dass wichtige wirtschaftliche Sektoren der Volkswirtschaft vertrauenswürdige Systeme implementieren sollten.[81] Gleichzeitig wurde verboten, dass TPMs ausländischer Hersteller durch lokale Unternehmen in chinesische Hardware verbaut werden durften.[82]

7.1.2 Die aktuelle Entwicklung

Die nationalen F&E-Anstrengungen decken nach Einschätzung der chinesischen Experten nahezu alle wesentlichen Entwicklungsbereiche von TC ab. Dabei werden einige Themenfelder aus Sicherheitsgründen stärker von der Politik, andere aus Wettbewerbsgründen stärker von den Unternehmen vorangetrieben. Aus der Sicht der politischen Administration gilt es dabei grundsätzlich, jedes Element der Wertschöpfungskette bzw. der technologischen Komponenten zu beherrschen und unter Sicherheitsgesichtspunkten neu zu entwickeln (vgl. Abbildung 7-1). Gleichzeitig sollen alle Anstrengungen und Investitionen an den folgenden Grundsätzen ausgerichtet werden:

81 Vgl. Administrative Measures on the on the Prevention of Classified Information Security (MPS, 2006).
82 Vgl. Provisions for Utilization of Commercial Cipher Products (OSCCA, 2007).

Abbildung 7-1: Trusted Computing in China: Schwerpunkte und Produkte



Quelle: Qing 2005 Keynote Speech bei der 20th CNITSEC Konferenz (Aug. 2005), ergänzt durch WIK-Consult

1. Sämtliche Kerneltechnologien sollen ausschließlich durch chinesische Firmen hergestellt werden.

2. In einigen Bereichen wie der Entwicklung von Ein- und Ausgabesystemen (BIOS) sowie bei Betriebssystemen sollen die technologischen Durchbrüche, die in diesen Bereichen in den letzten Jahren in China erreicht worden sind, durch weitere Anstrengungen vorangetrieben und im Rahmen der übrigen TC-Aktivitäten konsolidiert werden.

3. In denjenigen Feldern wie z. B. CPU-Entwicklung und Chipsets, bei denen der technologische Rückstand chinesischer Firmen als noch besonders groß betrachtet wird, sollen die F&E-Anstregungen mit nachrangiger Priorität verfolgt werden.

Vor diesem Hintergrund sind die F&E-Aktivitäten auf einige als wesentlich erachtete Bereiche konzentriert. Nach jahrelanger intensiver Förderung durch die Regierung sind mittlerweile die ersten Produkte wie z. B. das von Sinosun hergestellte TPM am nationalen Markt erhältlich.

Obwohl nach Einschätzung der Experten TC eine große Vielfalt von Produkten umfasst und auch für die meisten der übrigen Wirtschaftssektoren eine wichtige Technologie darstellen kann, konzentrieren sich die meisten Aktivitäten auf den Markt „sicherer“ Desktop Geräte. Dies ist vor allem vor dem Hintergrund zu sehen, dass die meisten Kunden für entsprechende Geräte aus dem staatlichen Sektor (Regierungsstellen, Militär, Bankwesen, öffentliche Versorger etc.) kommen, bei denen der Einsatz entsprechend ausgestatteter Geräte, wie oben bereits erwähnt, vorgeschrieben ist.

Für das Jahr 2008 wird der Markt für „sichere“ Personal Computer in China auf rund fünf Millionen Geräte geschätzt mit einem Gesamtinvestitionsvolumen von rund 800 Mio. Euro. Hiervon enfallen etwa 70% auf die Nachfrage aus dem öffentlichen Sektor, wovon wiederum 60% auf Regierungsstellen sowie 10% auf das Militär entfallen.

7.1.3 Entwicklung der rechtlichen Rahmenbedingungen

Alle Aspekte, die mit Trusted Computing zusammen hängen, fallen in den Kontext der Informationssicherheit, für die in China auf Regierungsebene mehrere Stellen zuständig sind. Hierzu gehören das Ministerium für die Informationsindustrie (Ministry of Information Industry (MII), das Ministerium für Wissenschaft und Technologie (Ministry of Science and Technology (MoST)), das Ministerium für öffentliche Sicherheit (Ministry of Public Security (MPS)) sowie verschiedene Behörden in anderen Ministerien, in deren Verantwortung das Management der Informationssysteme verschiedener Sektoren liegt.

Alle diese verschiedenen Aktivitäten werden koordiniert durch das Office of Informatisation, das institutionell auf höchster politischer Ebene beim Staatsrat angesiedelt ist und das für die Vorbereitung regulatorischer Maßnahmen sowie für die strategische Ausrichtung der IT-Sicherheitspolitik zuständig ist.

Unter dem Gesichtspunkt der Zuständigkeiten und der operationellen Umsetzung der IT-Sicherheitspolitik bestehen in Hinblick auf die Anbieter von Produkten sowie auf die Anwender unterschiedliche institutionelle Strukturen.

7.1.3.1.1 Regulierung der Angebotsseite

Zweifellos sind alle Anbieter von Hard- oder Software-Produkten in China verpflichtet, ihre Herstellungs- und Vermarktungsaktivitäten eng an den politischen Vorgaben auszurichten und werden hierbei von den staatlichen Stellen kontrolliert. Einen besonderen und für TC einschlägig relevanten Aspekt der Regulierung der Angebotsseite stellen jedoch die Aktivitäten des Office of State Commercial Cipher Administration (OSCCA) dar.

Die Hauptaufgabe des OSCCA besteht darin, alle Kernkomponenten, die in Verschlüsselungstechnologien verwendet werden, auf den Grand ihrer Zuverlässigkeit hin zu überprüfen. Um dieser Aufgabe gerecht zu werden, hat das OSCCA strikte Vorgaben für den gesamten Forschungs-, Entwicklungs- und Herstellungsprozess bis hin zu den Anwendungen entwickelt und wacht über deren Einhaltung:

- Generell gelten alle Verschlüsselungstechnologien als Staatsgeheimnis. Sowohl der Forschungs- und Entwicklungsprozess als auch die Vermarktung und die Nutzung werden ausschließlich von staatlichen Behörden kontrolliert und genehmigt (General Ordinance, 1999).

- OSCCA bestimmt und koordiniert alle F&E-Aktivitäten im Bereich kommerzieller Verschlüsselungsprodukte in China. Einschlägige F&E-Aktivitäten dürfen nur durch solche Organisationen oder Firmen durchgeführt werden, die durch OSCCA ausgewählt wurden. Es ist den entsprechenden Organisationen oder Firmen strikt untersagt, Personal mit fremder Staatsangehörigkeit einzustellen und zu beschäftigen (Provisions for R&D, 2005).

- Die industrielle Herstellung von Verschlüsselungsprodukten darf ebenfalls nur in solchen Firmen erfolgen, die durch OSCCA ausgewählt wurden und den enstprechenden Sicherheitsanforderungen entsprechen (Provisions for Manufacture, 2005).

- Chinesische Organisationen, Unternehmen oder Bürger dürfen nur solche Verschlüsselungsprodukte verwenden, die von OSCCA lizenziert wurden. Die Verwendung der in aller Regel nicht lizenzierten ausländischer Produkte ist strikt untersagt (Provisions for Utilization, 2007).

- Verschlüsselungsprodukte können nur bei Händlern erworben werden, die im Besitz einer staatlichen Konzession sind. Alle Produkte “developed and manufactured by foreign countries are forbidden to be sold in the territory of China” (Provisions for Sales, 2005).

OSCCA hat bisher insgesamt rund 300 Lizenzen an Firmen vergeben, die entsprechende Produkte vertreiben dürfen. Insgesamt drei Lizenzen wurden für den Verkauf von TPMs an Lenovo (SSX24), Sinosun (SSX 35) sowie Jetway (SSX 36) vergeben. Die Gründe in der geringen Anzahl von TPM-Lizenzen dürfte insbesondere im hohen Kontrollbestreben von OSCCA liegen. Zudem werden drei Lizenzen als “hinreichend für den Wettbewerb unter den Chip-Herstellern“ angesehen.

7.1.3.1.2 Regulierung der Nachfrageseite

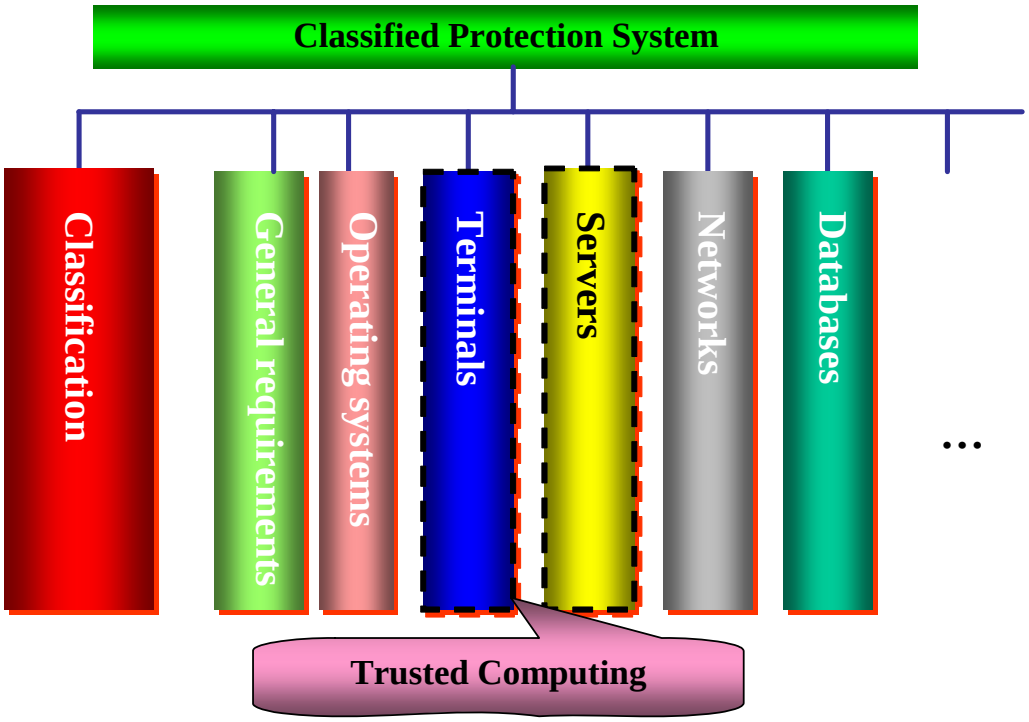
Das Ministerium für öffentliche Sicherheit (MPS) hat 2006 durch administrative Maßnahmen (Administrative Measures (2006)) ein Sicherheitssystem etabliert, das alle nationalen Informationssysteme in 5 Kategorien[83] in Bezug auf ihre Bedeutung für die nationale Sicherheit, das öffentliche Interesse, die soziale Ordnung sowie die wirtschaftliche Zuverlässigkeit einteilt. Diese Einteilung entspricht den unterschiedlichen Prioriäten und Stufen der Schutzstrategie. Die Stufen 3 bis 5 müssen zwangsläufig einem Zertifizierungs- und Monitoringprozess seitens des MPS unterworfen werden.[84] Diese Ebenen erfordern zwingend die Anwendung bestimmter Schutzmechanismen („trusted systems“). Die entsprechende Anweisung bildet im Rahmen eines Classified Protection System ein vollständiges Set von Sicherheitskomponenten ab, die bei der Implementierung und Anwendung Berücksichtigung zu finden haben. Hierbei ist TC als ein wichtiger Bestandteil vorgesehen (vgl. Abbildung 7-2).

---

83 Zu den fünf Ebenen des Schutzes von Informationssystemen gehören:
Ebene 1: Eigenständiger Schutz von Systemen, “whose damage doesn’t impair national security, social order or public interests.” The operator may protect the system autonomously according to national criteria and technical standards;
Ebene 2: Angeleiteter Schutz von Systemen, “whose damage slightly impairs social order or public interests, but no impact on national security.” The operator shall protect the system according to national criteria and technical standards, with asking for MPS’s guidance if necessary;
Ebene 3: Überwachter Schutz von wichtigen Informationssystemen “involving national security, social order or public interests whose damage may impair national security, social order or public interests.” The operator shall protect the system according to national criteria and technical standards. MPS and its offices supervise the protection and make inspection once a year;
Ebene 4: Obligatorischer Schutz für wichtige Informationssysteme “involving national security, social order or public interests whose damage severely impairs national security, social order or public interests.” The operator shall protect the system according to national criteria and technical standards. The protection is obligatorily supervised by MPS, and MPS makes inspection twice a year;
Ebene 5: Besonders kontrollierte Schutzmechanismen für bedeutende Informationssysteme “involving national security, social order or public interests whose damage extremely severely impairs national security, social order or public interests”. The operator shall protect the system according to national criteria and technical standards. The protection is supervised and inspected by the state-designated institutions.

84 Die folgenden Sektoren bzw. Anwendungsbereiche unterliegen dem Ziel einer obligatorischen Überwachung: Regierungsbehörden (Institutionen der Partei sowie alle offiziellen Regierungsstellen auf allen Ebenen), Institutionen des Finanzsektors, der Steuerbehörden, des Handels, der Telekommunikation, des Energie- und Versorgungssektors, des Transportsektors, der Medizin- und Notfallversorgung, des Erziehungssektors, der Forschung sowie der nationalen Verteidigung.

Abbildung 7-2: Trusted Computing als Teil des Classified Protection System



Quelle: Zhu (2005) Classified Security System, Annual Conference of China Computer Society

7.1.4 Gestaltungsansätze für Trusted Computing

Die Perspektive der Regierung

Bis zum Jahr 2005 waren die Aktivitäten zu TC eingebettet in den allgemeinen Bereich der Informationssicherheit und verteilten sich auf verschiedene Felder und Handlungsebenen. Je mehr sich jedoch mit der wachsenden Nutzung des Internet sowie der damit verbundenen Risiken die Bedeutung vertrauenswürdiger Plattformen für die nationale Industrie zeigte, um so stärker differenzierte und akzentuierte sich die Einstellung der Politik. Im 11. Fünf-Jahresplan (2006 - 2010) wurde die Bedeutung der Informationssicherheit stark hervorgehoben. Im Rahmen der diesen Plan begleitenden „National Strategies for Informatization (2006 – 2020)“, die der Staatsrat verfolgte, unterstrich die Zentralregierung erstmalig die besondere Bedeutung vertrauenswürdiger Systeme für die Umsetzung einer nationalen Sicherheitsstrategie.

Schon bald nach Verabschiedung des 11. Fünf-Jahresplans wurden folgende konkreten Maßnahmen umgesetzt:

- Im Jahr 2006 gab das Ministerium für die Informationsindustrie (MII) die Förderung von 10 Schlüsselprojekten bekannt[85], die im Rahmen des neuen Fünf-Jahresplanes durchgeführt werden sollten. TC wurde hierbei explizit als eine der Schlüsseltechnologien des 10. Projektes, das sich mit „Networks and Informations Security" befasste, genannt. Das MII unterstrich, dass es mit dieser Initiative insbesondere zur Verbreitung vertrauenswürdiger Systeme in der Industrie beitragen wollte. In den „favored topics of 2007" wurde verdeutlicht, dass im Rahmen der Innovationsförderung insbesondere kleinen und mittelständischen High-Tech-Unternehmen mehrere Mio. US$ sowie Mittel der lokalen Behörden zur Verfügung gestellt würden, wenn sie zu den F&E-Aktivitäten für TC beitragen würden.

- Die National Science Foundation als wichtigste Institution der Förderung der Grundlagenforschung an Universitäten sowie der Chinesischen Akademie der Wissenschaften (CAS), gab bekannt, dass sie im Rahmen des 11. Fünf-Jahresplans[86] die Entwicklung vertrauenswürdiger Plattformen in den Mittelpunkt ihrer Förderung zu stellen beabsichtigte. Dies bedeutete, dass für diesen Forschungsschwerpunkt Mittel in Höhe mehrerer Mio. US$ zur Verfügung gestellt wurden.

- Im Juli 2007 schließlich wurde im Rahmen der Projektförderung für den Forschungsschwerpunkt 863, der von MII unterstützt wurde zur allgemeinen Entwicklung von „technologies which are pivotal to the society and economy" TC als besonderer Schwerpunkt der "Special Projects"[87] implementiert. Mit dieser Schwerpunktsetzung ist ebenfalls eine Förderung in Höhe von mehreren Mio. US$ verbunden. Diese Mittel sollen noch in diesem Jahr für Projektvorschläge von Hochschulen und Unternehmen zur Verfügung gestellt werden.

- Bis 2010 sollen in allen Verwaltungsstellen des Landes sowie beim Militär nur noch Endgeräte zum Einsatz kommen, die auf Trusted Computing-Technologie basieren. Hiervon soll nicht nur die nationale Sicherheit profitieren, sondern insbesondere auch den Anbietern ein Schub in Hinblick auf die internationale Wettbewerbsfähigkeit gegeben werden.

---

85 Diese 10 Schlüsselprojekte umfassen: (1) Integrated Circuits; (2) Software; (3) Next Generation Mobile Communications; (4) Next Generation Internet; (5) Digital Broadcasting; (6) Broadband Communications; (7) High Performance Computing; (8) New Electronic Parts; (9) Telecom Universal Services; (10) Networks and Information Security.

86 Vgl. The 11th Five-Year Plan of National Science Foundation, http://www.nsfc.gov.cn.

87 Vgl. die Angaben zum Project „Next Generation High Trustworthy Internet Project". Approved News Release, July 2007, Ministry of Information Industry, http://www.most.gov.cn/kjbgz/200707/t20070705_50843.htm, Panel Meeting for the Next Generation High Trustworthy Internet Project Held in Beijing, http://www.most.gov.cn/eng/pressroom/200707/t20070711_50997.htm.

7.1.5 Die Perspektive der Forschungseinrichtungen

Die wissenschaftliche Grundlagenforschung zu vertrauenswürdigen Plattformen wird schwerpunktmäßig sowohl an den Hochschulen als auch an der CAS durchgeführt. In den vergangenen zehn Jahren gehörten Fragen der Informationssicherheit zu den wichtigsten Schwerpunkten der Informatik. Vor diesem Hintergrund ist es wenig erstaunlich, dass TC in den letzten Jahren zu einem der wichtigsten Kernpunkte der Forschungsaktivitäten an allen bedeutsamen Hochschulen avanciert ist. Die bekannteste Einrichtung hierbei ist das Department of Computer Sciences der Tsinghua University in Peking, welches mit ernormen personellen Anstrengungen die Forschungsaktivitäten zur Verbesserung der Sicherheit im Internet vorantreibt. Dort wird offenkundig auch an Strategien der Virtualisierung gearbeitet.

Als zweite Hochburg für TC-orientierte Forschung ist das Institute of Software Engineering der Chinesischen Akademie der Wissenschaften in Peking zu nennen, das nach Ansicht der Experten unter der Leitung von Prof. S. H. Qing das erste vertrauenswürdige Betriebssystem in China entwickelt hat.

7.1.6 Die Perspektive der Herstellerunternehmen

Entsprechend der Vorgaben von OSCCA dürfen sämtliche F&E-Aktivitäten, die auf die Entwicklung von Verschlüsselungsprodukten zielen, nur von Unternehmen durchgeführt werden, die hierfür zugelassen wurden. Dies schließt ein, dass die meisten dieser Unternehmen z. T. enge Kontakte zu einzelnen Hochschulen bzw. zur Chinesischen Akademie der Wissenschaften unterhalten. Solche Verbindungen dienen nicht zur effizienten Durchführung von F&E, sondern auch dem Know-how Transfer und der Umsetzung in konkrete vermarktungsfähige Produkte (vgl. Abb. 6-2).

Von besonderer Bedeutung für F&E im Bereich TC sind diejenigen Unternehmen, die bereits auf kommerzieller Basis TPMs entwickeln. Dies sind, wie oben bereits erwähnt, die Firmen Lenovo, Sinosun sowie Jetway, die durch OSCCA lizenziert worden sind. Dabei sind die Herangehensweisen dieser drei Akteure sehr unterschiedlich.

a) Lenovo

   Lenovo wurde 1984 von 11 Wissenschaftlern der Chinesischen Akademie der Wissenschaften gegründet und ist heute – nach der Übernahme von Geschäftsfeldern der US-amerikanischen Firma IBM – der drittgrößte Computer-Hersteller der Welt. Lenovo war das erste Unternehmen in China, das 2005 ein TPM mit dem Namen Hengzhi hergestellt hat, das in vollem Umfang mit dem Standard v1.2 der TCG kompatibel ist.

Allerdings wurde die Entwicklung dieses Hardware-Bausteins von den übrigen chinesischen Herstellerfirmen mit Zurückhaltung betrachtet. Schon wenige Monate später stellte das Unternehmen Tongfang den ersten PC vor, der mit einem TPM der Firma Sinosun ausgerüstet war. Hiermit scheint – zumindest aus heutiger Sicht – eine gewisse Vorentscheidung zugunsten des Produktes von Sinosun gefallen zu sein. Seit der Markteinführung des Tongfang-Computers verwenden alle einschlägigen Hersteller das TPM von Sinosun.[88]

Forschung und Entwicklung im Bereich TC erfolgen bei Lenovo Corporate R&D, das einem Joint Venture von Lenovo sowie der Chinesischen Akademie der Wissenschaften entstammt. Die Einzelheiten dieser Aktivitäten sind öffentlich nicht zugänglich, allerdings geben einzelne Veröffentlichungen von Lenovo Hinweise darauf, dass dort ein ähnlicher Ansatz der Etablierung einer vollständigen Vertrauenskette verfolgt wird wie in Europa oder den USA.[89]

In den Veröffentlichungen von Lenovo wird argumentiert, dass der heutige Mechanismus der Vertrauensgenerierung zu statisch ist angesichts der wachsenden Komplexität der Systemumgebung und der Anwendungen. Statt dessen wird ein Ansatz einer “erweiterten, vollständigen Vertrauenskette verfolgt, der eine Beobachtung des Verhaltens von Software in Echtzeit ermöglicht. Dies wird als eine Schlüssellösung betrachtet, um die Vertrauenswürdigkeit in dynamisch veränderlichen Systemen sicher zu stellen.

b) Sinosun

Erst 1995 gegründet, gehört Sinosun heute zu den wichtigsten Herstellern und Anbietern von Sicherheitslösungen im Hard- und Software-Bereich. Sinosun hat sein erstes TPM 2005 vorgestellt und unternimmt seitdem erhebliche Anstrengungen zu seiner Vermarktung. Durch die Bestätigung der Konformanz dieses TPM mit dem TCG Standard v1.2 sowie der Interoperabilität mit den Produkten von Intel und Microsoft wurden früh die Weichen für den Markterfolg gestellt. Durch seine starke Fokussierung auf IT-Sicherheit wird Sinosun von den übrigen Unternehmen im Markt eher als spezialisierter Nischenanbieter denn als Wettbewerber angesehen. Angesichts der durchgreifenden Regulierung durch OSCCA zur Erhöhung der Sicherheit sind die TPM Chips von Sinosun heute auf den meisten Motherboards von PCs, die für den chinesischen Markt gefertigt wurden, zu finden.[90]

---

88 Vgl. eNet News, June 2005, sowie eigene Recherchen auf den Websites der wichtigsten chinesischen Computerhersteller.

89 Vgl. Wu (2006), Establishing the T-Chain Centered Architecture of Trusted Computing, Technical Report, Lenovo Corporate of Research and Development.

90 Vgl. http://www.sinosun.com/about/.

c) Jetway

Jetway ist eine stark wachsende Firma im Markt für IT-Sicherheit, die erst Ende der 90er Jahre als Joint Venture von der Universität Wuhan sowie von den Instituten der Chinesischen Akademie der Wissenschaften in Wuhan gegründet wurde. Jetway konzentrierte seine Aktivitäten schon früh auf die Entwicklung von TPMs und stellte seine ersten Produkte bereits Mitte 2004 einer breiteren Öffentlichkeit vor. Der technologische Ansatz von Jetway unterscheidet sich jedoch deutlich von Lenovo und Sinosun und seine TPMs sind nicht kompatibel mit den Standards der TCG.

Gemäß der Unternehmensphilosophie von Jetway werden sämtliche Komponenten einschließlich Hardware, BIOS, Betriebssysteme sowie Anwendungssoftware neu entwickelt, um „truly trustable“ zu sein. In jüngster Zeit wurde das Portfolio von Jetway durch Eigenentwicklungen im Bereich „vertrauenswürdiger“ Server sowie Netzwerkkomponenten ergänzt bzw. erweitert. Die eigenständige Vorgehensweise von Jetway hat mittlerweile auch das Interesse des chinesischen Militärs geweckt, so dass Jetway davon ausgeht, in Kürze Aufträge im dreistelligen Mio. US$-Bereich zu erhalten. Jetway konzediert, dass die Entwicklungsphilosphie des Unternehmens häufig mit großen Problemen verbunden ist und es nicht eben leicht erscheint, das Vertrauen nationaler Partner- und Anwenderfirmen zu bekommen. Derzeit ist keine Firma bekannt, der die TPMs von Jetway verwendet.[91]

7.1.7 Die Rolle anderer Hardware- und PC-Hersteller

Die Firma Great Wall ist ein staatliches Unternehmen, das 1986 gegründet wurde und den ersten x86-basierten Rechner in China entwickelte. Great Wall gehört heute zu den größten Lieferanten von Computerausrüstungen für die Regierung und die Armee. Great Wall entwickelte die erste Universal Extensible Firmware Interface-BIOS und verfügt über großes Know-how im Bereich der Speichertechnologie. Seine F&E-Aktivitäten im Bereich vertrauenswürdiger Plattformen begann Great Wall im Jahre 2002 und stellte eine erste Generation von entsprechenden Produkten bereits drei Jahre später vor. Die erste Produktgeneration durchlief seither einen großen Feldtest durch den Einsatz von über 50.000 Geräten bei Regierungs- und Armee-Stellen.[92]

Am 8. August 2007 stellte Great Wall seine 2. Generation von Produkten vor, die nach Verlautbarung des Unternehmens den höchsten Grad an Sicherheit der derzeit auf dem chinesischen Markt erhältlichen Produkte aufweisen. Mit Ausnahme der CPU sind alle

---

91 Vgl. China Computer World, Oct. 2005.
92 Vgl. CCID News, Aug. 2007.

Komponenten chinesischen Ursprungs,[93] das TPM stammt von Sinosun und das Betriebssystem basiert auf einer adaptierten Version von Linux. Die besonders „gehärtete“ Festplatte wurde von Great Wall hergestellt und erlaubt es, darauf - physikalisch separiert - Daten von unterschiedlichen Nutzern sicher zu speichern.

Alle großen Hersteller haben heute „vertrauenswürdige“ Rechner in ihrem Produktportfolio, die unter dem Label „Safe PC“ vermarktet werden. Gleichwohl muss davon ausgegangen werden, dass, bis auf die Tatsache, dass alle diese Geräte ein TPM besitzen, die einzelnen Lösungen sich sehr stark voneinander unterscheiden. So bieten einige Rechner für Einsteiger als Zugangsbarriere eine biometrische Schnittsstelle für das Lesen des Fingerabdrucks, während im High-End-Bereich spezielle Lösungen angeboten werden, die entsprechend an die jeweiligen Sicherheitsanforderungen eines Nutzers angepasst werden. Ein Wettbewerber von Great Wall, die Firma Inspur, kritisiert daher, dass vielfach im chinesischen Markt eher ein Konzept als ein Produkt mit fest definierten Eigenschaften verkauft wird.[94]

Neben Great Wall gibt es eine Reihe weiterer Hard- und Software-Hersteller, die sich im Bereich TC engagieren. Die Aktivitäten dieser Unternehmen wurden in der Vergangenheit häufig durch das Ministerium für Wissenschaft und Technologie (MoST) gefördert und konzentrieren sich u. a. auf folgende Bereiche:

7.1.7.1 Entwicklung eines BIOS

Da ein BIOS in Zusammenhang mit dem Einsatz eine wichtige Rolle spielt, wurde dieser Bereich speziell gefördert. Besonders der offene Standard UEFI erlaubt es neuen Firmen, in diesem Feld aktiv zu werden, was dazu geführt hat, dass sich heute eine Reihe von Entwicklern mit ihren Lösungen im Wettbewerb befinden. Entsprechende Produkte sind z. B. erhältlich über Great Wall, Nanjing Bysoft etc.

7.1.7.2 Betriebssysteme

Das Betriebssystem Redflag, das von Instituten der Chinesischen Akademie der Wissenschaften gefördert und entwickelt wurde, stellt heute das dominierende Betriebssystem in China dar. Basierend auf Linux besitzt Redflag einen eigenen, in China entwickelten Kernel. In allen Bereichen, in denen hohe Sicherheitsanforderungen bestehen, kommt als Betriebssystem nur Redflag in Betracht.

---

93 Vgl. News Release, Aug. 2007, Great Wall Group.
94 Vgl. China Network World Weekly, No. 12, 2006.

7.1.7.3 Vertrauenswürdige Netzwerke

Während der Bereich von Endgeräte-bezogenen Hardware- und Software-Lösungen bereits auf einen gewissen historischen Vorlauf, eine Vielzahl von Akteuren und Produkten blicken kann, sind vertrauenswürdige Netzwerk-bezogene Lösungen ein Bereich, in dem sich heute zahlreiche Start-up-Unternehmen bewegen. Da davon auszugehen ist, dass in China in den nächsten Jahren ein großer Teil der vorhandenen Netzwerk-Infrastruktur mit Lösungen ersetzt wird, die klassifizierten Sicherheitsanforderungen entsprechen müssen, entsteht hier eine große Nachfrage nach vertrauenswürdigen Infrastrukturen.

7.1.8 Die China Trusted Computing Group

Die China Trusted Computing Group wurde im Januar 2005 ins Leben gerufen, um zum einen mit den Vertretern aller involvierten Ministerien, der Forschungseinrichtungen sowie der nationalen Hersteller die Anforderungen an und die Zielsetzungen einer nationalen TC-Politik zu formulieren. Auf der anderen Seite sollte die China Trusted Computing Group die Aufgabe übernehmen, insbesondere auch den Austausch zwischen den Unternehmen zu verbessern und deren divergierende Aktivitäten zu koordinieren.

Schon nach kurzer Zeit wurde deutlich, dass es mit erheblichen Schwierigkeiten verbunden war, eine einheitliche Ausrichtung einer nationalen TC-Politik zu formulieren für einen Bereich, der heterogen und fragmentiert war und teilweise von den widersprüchlichen Interessenlagen einer nationalen versus einer internationalen Ausrichtung geprägt wurde. Vor diesem Hintergrund verwundert es nicht, dass es der China Trusted Computing Group nicht gelang, einen verbindlichen Fahrplan für den weiteren Abstimmungs- und Standardisierungsprozess zu formulieren.[95]

Seither wurden nur wenige neue Informationen seitens der CTCG bekannt. Experten vermuten jedoch, dass die Ereignisse von 2006 dazu beigetragen haben, dass diese Organisation ihre Anstrengungen deutlich intensiviert hat. Generell ist davon auszugehen, dass die CTCG die Aktivitäten der TCG in ihre Arbeit mit einbezieht und deshalb auch Lenovo sowie Sinosun an den Standardisierungsaktivitäten beteiligt nach dem Motto: Es macht ökonomisch wie politisch wenig Sinn, einen technologisch vollständig eigenen Weg zu gehen. Für diese Sichtweise steht auch, dass die OSCCA den v1.2 Standard verwendet, um die Konformanz der im Land hergestellten TPMs zu überprüfen. Chinesische Experten befürworten daher auch die Mitarbeit der CTCG bei der TCG.

---

95 Vgl. http://www.tcgchina.com.

Andere Stimmen hingegen votieren für eine Strategie, nach der alle Sicherheitsrelevanten Schlüsseltechnologien in China hergestellt werden sollten und die „Root of Trust“ ausschließlich in nationaler Eigenregie entwickelt werden sollte. Vor diesem Hintergrund ist davon auszugehen, dass der Löwenanteil der TCG-Standards in die chinesischen Aktivitäten einfließen wird und nur ein kleiner Teil in China selbst entwickelt werden wird.

7.1.9 Trusted Computing als Gegenstand der Politik und der öffentlichen Meinung

In Bezug auf die langsame Entstehung des Marktes für TC-Produkte und die Rolle der TCG ist das chinesische Verhalten stark von der Befürchtung geprägt, dass TC ein Schlüssel sein könnte, um chinesische Firmen aus den internationalen Märkten für Hard- und Softwareprodukte zu drängen.[96] Gleichzeitig werden die enormen industriepolitischen Chancen von TC gesehen, die allgemeine Informationssicherheit zu erhöhen und chinesischen Firmen den Zugang zu den entsprechenden Märkten offen zu halten bzw. zu sichern. Vor diesem Hintergrund werden die chinesischen Unternehmen nicht müde, im Rahmen der Diskussion über TC zugleich Forderungen nach Schutzmaßnahmen zur Abwehr ausländischer Wettbewerber zu artikulieren.[97]

Während also TC in der Politik sowie im akademischen und industriellen Sektor eine große Rolle spielt, hat es in China - im Gegensatz zur westlichen Welt - bisher so gut wie keine öffentliche Debatte über TC gegeben. Die potenzielle Bedrohung individueller Nutzungsrechte sowie der Privatheit durch TPMs, wie sie in den westlichen Ländern um die Jahrtausendwende intensiv diskutiert worden ist, ist bisher weder Gegenstand öffentlicher Diskussionen noch Gegenstand der Politik. Die im Rahmen dieser Untersuchung durchgeführte (begrenzte) Analyse von Online-Medien, Webforen, Blogs oder elektronischen Bulletins ergibt praktisch keinerlei Hinweise darauf, dass dieses Thema wahrgenommen, geschweige denn reflektiert oder kontrovers diskutiert wird.[98]

Eine einzige Ausnahme bildet, wenn auch sehr begrenzt, das Thema DRM. DRM wird jedoch weniger in Hinblick auf die Durchsetzung nationaler Rechteinhaber diskutiert als vielmehr als Versuch westlicher Firmen wahrgenommen, ihre Rechte durchzusetzen und ihre Marktmacht zu erhöhen.[99]

---

96 Vgl. Qing (2005), Keynote Speech on the Annual Conference of China Information Society.
97 Vgl. Wang, Stop the Foreign Firms’ Fraud! in Herald of China Hi-Tech Industries, April 17, 2006.
98 Vgl. z. B. CCID News, März 2007.
99 Vgl. http://www.stdaily.com/gb/misc/2004-11/24/content_327428.htm.

7.1.10 Die Diskussion um TPM als Verschlüsselungstool

Im April 2006 wurde durch offizielle Stellen die Nachricht verbreitet, dass die US-amerikanischen Firmen Hewlett-Packard und Dell Personal Computer im chinesischen Markt verkauften, die ein TPM enthielten, welches im Ausland hergestellt worden war und wahrscheinlich gegen die Verordnungen der OSCCA verstieß. Weitere Untersuchungen zeigten, dass diese Firmen für die Nutzer entsprechende Software bereitstellten, um das TPM aktivieren zu können. Hewlett-Packard und Dell argumentierten dagegen, dass das TPM ausschließlich zu Zwecken der Nutzeridentifikation und nicht zur Verschlüsselung genutzt werden könnte.[100]

Allerdings wurde diese Argumentation von Wissenschaftlern sowie Marktforschungsinstituten kritisiert mit dem Hinweis, dass Produkte mit TPM eine Bedrohung der nationalen Industrie darstellten und verlangten eine Verschärfung der bestehenden Regulierung.[101] In diesem Verfahren stellte OSCCA schließlich fest, dass TPM Chips als kommerzielles Verschlüsselungstool zu betrachten sei.[102] Kurz danach wurde eine neue Anordnung veröffentlich, nach der es chinesischen Nutzern verboten wurde, ausländische Verschlüsselungsprodukte zu verwenden.[103]

HP sowie Dell stellten darauf hin den Verkauf ihrer Rechner mit TPM ein. Gleichzeitig boten nun ASUS sowie SONY Rechner mit TPM an, die von Sinosun hergestellt worden waren. Intel und Microsoft schließlich unterstützten Lenovo und Sinosun bei der Durchführung von Kompatibilitätstests für ihre TPMs in der Hoffnung, hierdurch ihre Präsenz auf dem chinesischen Markt absichern bzw. ausweiten zu können.

7.1.11 Entwicklung der Trusted Computing - Diskussion in China

Seit die Diskussion über TC in den letzten Jahren zunehmend an Bedeutung gewonnen hat, gelingt es der CTCG immer weniger, die Mitwirkung an den weiteren Standardisierungsaktivitäten auf einen kleinen, exklusiven Kreis von Akteuren zu beschränken. Obwohl argumentiert wird, dass es sich nach Aussagen der CTCG um einen Industriestandard handelt, drängen zunehmend auch andere Interessenten in die TC-Arena.[104]

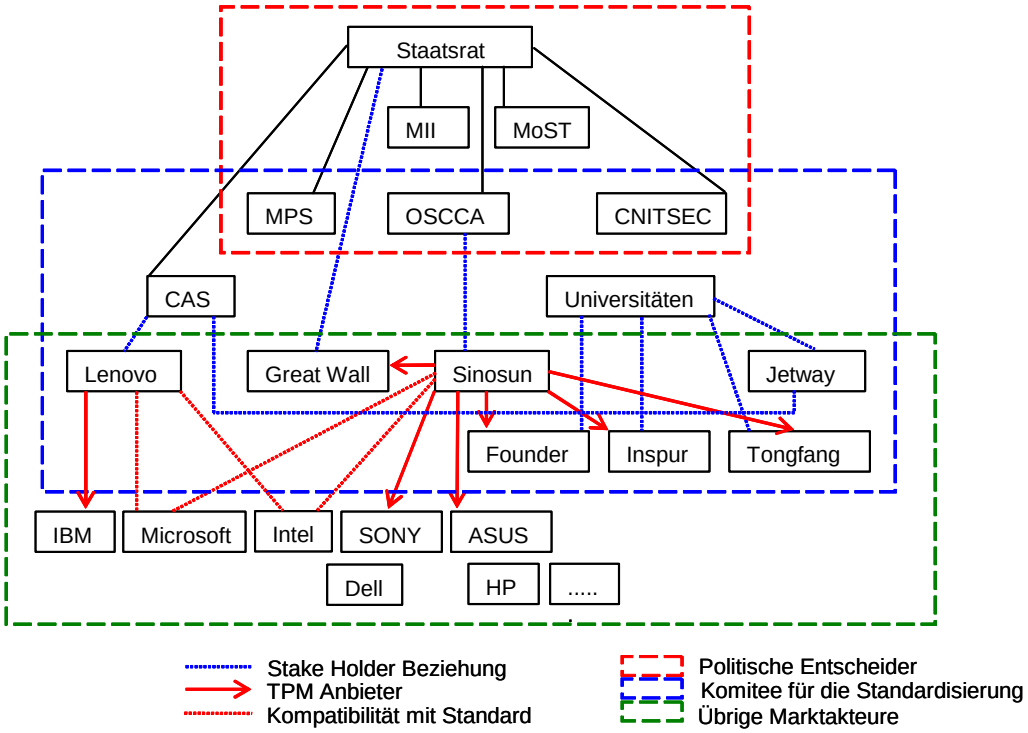
---

100 Vgl. China Computer World, May 8, 2006.
101 Vgl. Herald of China Hi-Tech Industries, April 17, 2006.
102 Vgl. Li, CCW Research, May 2006.
103 Vgl. China Times for Industry and Commerce, March 15, 2006.
104 Vgl. Fußnote 94, in der Bezug genommen wird auf das Interview mit dem stellvertretenden Direktor Yanwen Qu (Deputy Director of CTCG, Professor der Peking University). In diesem Interview wird deutlich gemacht, dass die mit TC verbundenen Aspekte der nationalen Sicherheit der Regierung einen wichtigen Anreiz geben, sich in den Standardisierungsprozess einzumischen. Dieses Engagement der Regierung, das durchaus als industriepolitisches Argument zu Gunsten der nationalen Unternehmen interpretiert werden kann, wird künftig mit großer Sicherheit zu Problemen beim grenzüberschreitenden Warenaustausch führen. Vor diesem Hintergrund schweigen die Ministerien über ihre konkrete Einflussnahme auf die CTCG, während die CTCG nicht müde wird zu betonen, dass ihre Aktivitäten ausschließlich industriepolitisch motiviert sind.

Angesichts der vielfältigen Ausgründungen von entsprechend spezialisierten Unternehmen durch die Hochschulen des Landes ist die Zahl der Akteure in den letzten Jahren stark angewachsen. Gleichzeitig haben die Verflechtungen mit den verschiedenen politischen Institutionen und deren Einflussnahmen zugenommen.

Diese Entwicklung lässt es sehr unwahrscheinlich erscheinen, dass die weiteren Standardisierungsaktivitäten sich nur an ökonomischen bzw. industriepolitischen Rationalitäten orientieren. Die nachfolgende Abbildung (vgl. Abb. 5-3) gibt eine Übersicht über die Vielzahl der Akteure in der TC-Arena sowie deren Verbindungen untereinander.

Abbildung 7-3: Verflechtungen und Beziehungen in der TC-Arena



Quelle: WIK-Consult

Die wesentlichsten Spannungen bzw. Konflikte innerhalb der TC-Arena bestehen vor allem zwischen den chinesischen Chip-Herstellern. Der Hersteller Lenovo, dem weltweite Expansionsbestrebungen nachgesagt werden, geht davon aus, dass in einem „Trusted System“ das Zusammenspiel von Hardware und Betriebssystem so organisiert werden muss, dass ein möglichst hohes Maß an Kompatibilität mit den Produkten anderer, i. e. ausländischer Hersteller gegeben ist bzw. sich realisieren läßt.

Jetway verfolgt demgegenüber in Abstimmung mit der Regierung gezielt einen proprietären Weg der „Nicht-Kompatibilität“ mit der Zielsetzung, dass jede TC Hardware (die auf einem in China hergestellten Kernel basiert) die alleinigen Zugriffsrechte auf das Betriebssystem sowie darauf aufsetzende Applikationen haben sollte.

Sinosun in seiner Rolle Chip-Produzent hingegen verweist darauf, dass zunächst die Entwicklung der Standards vorangetrieben werden sollte. Diese Auseinandersetzungen werden als erhebliche Belastung für die Arbeit CTCG angesehen, die es ihr manchmal erschweren, “to define the scope of TC in the standards”.[105]

7.1.12 Zwischenfazit

- TC wird in China als eine sehr bedeutende Innovation angesehen, die es der chinesischen Regierung ermöglicht, auf der einen Seite mit ihrer Hilfe einen Beitrag zur Verwirklichung einer sowohl nach innen als auch nach außen gerichteten nationalen Sicherheitsstrategie zu leisten. Auf der anderen Seite wird TC als eine bedeutende Chance angesehen, die Wettbewerbsfähigkeit der nationalen Hard- und Software-Hersteller zu erhöhen. Da die politischen Entscheidungsträger bzw. Ministerien, die wissenschaftlichen Institutionen sowie alle wichtigen nationalen Unternehmen institutionell eng miteinander verflochten sind, erfolgt die Koordination zwischen allen Beteiligten sehr engmaschig.

- Der Staat stellt zudem große Summen bereit, um die angestoßenen F&E-Prozesse zu beschleunigen. Insgesamt bildet TC eines der wichtigsten Schlüsselelemente in den nationalen IT-Forschungsprogrammen. Deshalb ist damit zu rechnen, dass TC in den nächsten Jahren sowohl im öffentlichen als auch im privaten Bereich eine immer größere Rolle spielen wird.

- Gleichwohl wird TC derzeit fast ausschließlich unter Sicherheitsaspekten betrachtet, da die anderen Dimensionen bzw. Funktionalitäten bislang eher noch eine untergeordnete Rolle spielen. Aspekte wie der Schutz der Privatspäre, DRM oder die Rolle von OSS werden daher erst stärker in den Blickpunkt rücken, wenn die Industrie die vor ihr liegenden technischen und organisatorischen Hürden überwunden hat und es im internationalen Bereich Entwicklungen gibt, die auch für China Bedeutung bekommen könnten.

- In der Sicht deutscher Experten wird darauf verwiesen, dass die Rolle Chinas im Bereich TC - wie auch in vielen anderen Industriesektoren - keinesfalls unterschätzt werden darf. Auf Grund der Bereitschaft, große Ressourcen und Man Power in die als strategisch relevant bewerteten Bereiche zu investieren, ist der

---

105 Vgl. Sina Technology, April 26, 2005.

Anschluss an die Weltspitze etwa bei der Entwicklung eines Mikrokernels, der Entwicklung bzw. der Anpassung der Betriebssysteme, bei OSS oder bei Virtualisierung schon in wenigen Jahren zu erwarten. Der strategischen Zielsetzung, die gesamte Wertschöpfungskette der ITK-Hard- und Software in nationaler Eigenregie entwickeln zu können, ist daher eine große Bedeutung für die künftige Rolle Chinas in diesem Marktsegment beizumessen. Dies schließt insbesondere auch alle Aspekte der IT-Sicherheit sowie von TC ein. Aktuell jedoch wird noch ein gewisser Nachholbedarf konstatiert und der zeitliche Abstand auf etwa drei bis vier Jahre taxiert.

- Besonders hervorzuheben ist die chinesische Doppelstrategie, eigene, nicht mit der TCG kompatible Standards für nationale Zwecke zu entwickeln und gleichzeitig bei der TCG mitzuarbeiten, um die Wettbewerbsfähigkeit der nationalen Hersteller in den internationalen Märkten zu sichern.

7.2 Trusted Computing in den USA

Die in Kapitel 4 dargestellte Genese von Trusted Computing hat verdeutlicht, dass alle TC betreffenden Aktivitäten – wie auch fast alle übrigen Aspekte der weltweiten Hard- und Softwareherstellung – maßgeblich von US-amerikanischen Unternehmen initiiert, beeinflusst oder vorangetrieben werden. Insofern ist es wenig überraschend, dass auch in den USA die Entwicklungsarbeiten im Bereich Trusted Computing von den weltweit führenden großen US-amerikanischen IT-Unternehmen dominiert werden.

Die privatwirtschaftliche Trusted Computing Group – TCG (vormals TCPA – Trusted Computing Platform Alliance), eine Initiative der heimischen Industrie zur Entwicklung hardwarebasierter Sicherheitssysteme, wurde, nicht zuletzt auf Drängen anderer ausländischer Unternehmen, zwar nach und nach ausgeweitet, die maßgeblichen Akteure bleiben bis heute jedoch US-Firmen.

Dabei überwiegen, ganz im Gegensatz zu China, nicht national-strategische Motive, sondern ganz pragmatische Aspekte des Schutzes von Geschäftsinteressen das Verhalten der industriellen Akteure. So gelten entsprechend der Einschätzung der im Rahmen der Studie befragten Experten - wie auch schon vor einigen Jahren - als treibende Kräfte für das Engagement dieser Unternehmen zum einen die Eindämmung illegaler Kopien von Software sowie von digitalen Medieninhalten (Video, Audio). Zum anderen wird der Suche nach einem allumfassenden Schutz vor Malware, Angriffen oder DoS-Attacken eine immer wichtigere Bedeutung beigemessen.

Von Regierungsseite scheint das „Projekt“ TC (zumindest) nicht (erkennbar) offiziell gefördert zu werden. Für diese Einschätzung spricht einerseits, dass die US-amerikanische Beschaffungs- und Anwendungsphilosophie für den öffentlichen Sektor in der Vergangenheit eindeutig auf Commercials of the Shelf (COTS), also Produkten

und Anwendungen für den Massenmarkt basierte. Andererseits ist bekannt, dass die allerersten Initiativen zur Entwicklung und Implementierung von vertrauenswürdiger Hardware von den US-amerikanischen Militärs ausgingen.

Ferner ist davon auszugehen, dass Behörden wie vor allem die National Security Agency (NSA) die Arbeit der IT-Industrie begleiten und im konkreten Fall auch unterstützend tätig sind. Die Standardisierungsbehörde NIST (National Institute of Standards and Technology) ist zwar nicht direkt in den Standardisierungsprozess der TCG selbst involviert, steht jedoch in enger Verbindung zu den Akteuren, finanziert einschlägige Forschungsprojekte und verfolgt nach Einschätzung der Experten die Entwicklungsarbeiten und die Fortschritte der TC-Standardisierung mit großem Interesse.

Es ist vor diesem Hintergrund nicht unbedingt als Widerspruch zu werten, dass die Debatte um die wettbewerblichen, gesellschaftlichen und politischen Implikationen von TC für die geschäftlichen und privaten PC-Anwender in den USA frühzeitiger als in Europa begonnen hat und insbesondere von der Internet-Community lange Zeit sehr kritisch geführt wurde. Bekannte Verbraucher- und Datenschutzverbände wie z. B. die Electronic Frontier Foundation (EFF) haben früh und mit großer Intensität auf die Risiken von TC hingewiesen und es ist nicht auszuschließen, dass sie durch ihre Veröffentlichungen die Diskussion in anderen Ländern wie etwa in Deutschland angestoßen bzw. mit wichtigen Impulsen versorgt haben. So z. B. beziehen sich bestimmte Stellungnahmen des Chaos Computer Clubs (CCC) in Deutschland explizit auf entsprechende Argumentationen in den USA.

7.2.1 Kurze Darstellung des zeitlichen Ablaufs

In den USA wurde bereits 1997 das ursprüngliche Konzept hardware-gesicherter TC-Systeme von für das US-Militär tätigen Wissenschaftlern entworfen. Ein Teil der Autoren war zuvor für die NSA tätig. Aus dem Konzept entstand im Jahr 2001 ein Patent mit dem Namen „Secure and Reliable Bootstrap Architecture“.[106]

Der Chip-Hersteller Intel initiierte in den 90er Jahren im Zusammenhang mit Plänen zu einem neuen, sichereren Pentium-Chip ein Konsortium mit Microsoft und anderen Unternehmen (Compac/Hewlett-Packard, IBM). Diese Trusted Computer Platform Alliance (TCPA) wurde im Jahr 2003 in die Trusted Computing Group (TCG) umgewandelt. Heute besteht die Gruppe nach wie vor aus den Initiatoren Intel, Microsoft, Hewlett-Packard und IBM. Hinzu kamen der Chiphersteller AMD, der Soft- und Hardware-Hersteller Sun und die nicht-US-Unternehmen Infineon (AG in Streubesitz) und Lenovo (China) als sog. Promotoren.

---

106 Bill Arbaugh, Dave Farber und Jonathan Smith “A Secure and Reliable Bootstrap Architecture”, IEEE Symposium on Security and Privacy (1997), S. 65-71; US-Patent “Secure and Reliable Bootstrap Architecture”, U.S. Patent No. 6,185,678, February 6th, 2001, zit. nach Ross Andersson, Trusted Computing FAQ 1.1, http://moon.hipjoint.de/tcpa-palladium-faq-de.html.

Die Spezifikation 1.2 des Trusted Platform Module (TPM) gibt 2004 auch für die US-Unternehmen den Startschuss für die Produktion von Sicherheitschips. Die erste erfolgreiche TPM Spezifikation Version 1.1b wird nach und nach von Produkten, die der Spezifikation 1.2 entsprechen, verdrängt. Da US-amerikanische Unternehmen in vielen weiteren Bereichen und Produkten der IT-Wertschöpfungskette die Marktführerschaft besitzen oder anstreben, erscheint es folgerichtig, dass von diesen die Spezifikation für Mobilfunkgeräte, Speicherelemente, Server, Peripheriegeräte und IT-Infrastruktur vorangetrieben wird. So wurde z. B. bereits im Jahr 2005 eine Spezifikation für TPM für den wichtigen Bereich des Servermarktes vorgestellt. Außerdem wurde eine TNC (Trusted Network Connect) Architektur vorgestellt und eine Reihe von offenen Spezifikationen für Produkte, die diese unterstützen. Modifizierte Spezifikationen für Java und VoIP existieren inzwischen ebenfalls.

Das besondere Interesse US-amerikanischer Hersteller an TC zeigt sich u. a. auch darin, dass fast die Hälfte der in der TCG mitwirkenden Unternehmen, die als Kontributoren und Adoptoren in der TCG engagiert sind, aus den USA stammen. In unseren Expertengesprächen wurde die Erwartung unterstrichen, mit Hilfe der TC-Technologie auf internationalen Märkten den Schutz des geistigen Eigentums verteidigen zu können.

7.2.2 Derzeitiger Stand von Trusted Computing im Überblick

Aus der Sicht der US-Experten sind es in erster Linie US-Unternehmen, die in der Forschung und Entwicklung von TC Produkten führend sind und diese seit 2004 auch verstärkt auf den Markt bringen. Auch in der Nutzung von TPMs und weiteren (noch zu implementierenden) TC Standards werden die USA auf Grund der Marktmacht der US-Unternehmen sowie der zahlenmäßig hohen Verbreitung dieser Produkte künftig international maßgeblich sein. Für diese Einschätzung gibt es zahlreiche Indizien:

- Desktops und Notebooks in den USA werden heute z. B. von den Herstellern wie Hewlett-Packard, IBM oder Dell beinahe standardmäßig mit TPMs ausgestattet. Hewlett-Packard etwa vertreibt seine Notebooks der Serie D530, NC6000, NC8000 oder NW 8000 mit TPMs von Infineon. IBM vermarktet Notebooks der Serie NetVista mit TPMs der Firma National Semiconductor (PC 21100 Safekeeper). Der Hersteller Dell etwa baut in die Notebook-Serie „Latitude“ (X1, D419, D610, D810), die Mobile Workstations „Precision“ (M20, M70) sowie das Desktop System „Optiplex“ (G280) TPMs ein. Entsprechend sind Software-Pakete mit Applikationen für Daten- und Dateienverschlüsselung, sichere E-Mails, Single-Sign-On, Speicherung von Zertifikaten und Passwörtern sind verfügbar, ebenso Server mit TPMs.

- Die führenden Chip-Hersteller aus den USA wie Intel und AMD bieten Einzellösungen und integrierte Lösungen für Desktops und Notebooks an sowie für Server. Um Kostenvorteile aus den Economies of Scale zu erlangen, gehen die be-

fragten Experten davon aus, dass die Chip-Hersteller ein großes Interesse haben, TPMs in Chipsätze oder CPUs zu integrieren.

- Die TPM-Spezifikationen wurden erfolgreich auf den Servermarkt ausgeweitet. US-Hersteller haben Server entwickelt, die die Funktionalität besitzen, eine sichere Verbindung zwischen Client und Server nach dem TC-Prinzip zu gewährleisten. Diese bieten zudem inzwischen einen Mindestschutz gegen das Ausspähen des Server-Speichers.

- Die erste Anwendung für TNC (Trusted Network Connect) Architektur im Bereich Telemedizin wurde 2004 in den USA vorgestellt. Erste TNC-Produkte wie z. B. Switches, werden seit 2001 in den USA entwickelt und produziert. Das US-Softwareunternehmen Microsoft stellte vor zwei Jahren eine mit TNC interoperable Lösung für Microsofts Network Access Protection (NAP) Architektur vor.

- Auf bedeutsamen Messen und Kongressen in den USA wie z. B. der Interop Las Vegas und der RSA Konferenz werden regelmäßig wichtige Entwicklungen der TC vorgestellt und diskutiert. Dies wird von Branchenexperten als ein Beleg für die wichtige Rolle der US-Unternehmen auf dem Gebiet von Trusted Computing eingeschätzt. Da diese Messen insbesondere auf die Kommunikation mit wichtigen Anwendergruppen zielen, gilt dies als eine wichtige Form des Know-how Transfers.

- Es gibt Hinweise, dass die Interoperabilität auch bei US-Produkten noch nicht umfassend gewährleistet (z. B. bei TPM und TNC Lösungen) ist. Wiederholte Appelle bei solchen Veranstaltungen machen deutlich, wie ernst dieser Aspekte für eine vollständige Marktdurchdringung eingeschätzt wird.

7.2.3 Regulatorische Rahmenbedingungen

In den USA werden von Regierungsseite keine (erkennbaren) regulatorischen Aktivitäten zur Unterstützung der Verbreitung von TC unternommen. Die Industrieunternehmen finden ein innovationsfreundliches Klima vor, in dem das Motto: „Was den Unternehmen nutzt, nutzt den USA“ maßgeblich für die Politik der öffentlichen Hand ist. Gemäß dieser Philosophie werden Standards entwickelt, um sie im Wettbewerb in Produkte umzusetzen bzw. um mit ihrer Hilfe Wettbewerbsvorteile auf internationalen Märkten zu erzielen.

Ein wichtige treibende Kraft in diesem Zusammenhang sind die US-Armee sowie das Verteidigungsministerium, deren Agenda kontinuierlich von der Forderung nach verbesserter IT-Sicherheit bestimmt wird. Es ist auf Grund der Experteneinschätzung zu vermuten, dass es in diesem Bereich zahlreiche TC-relevante F&E-Aktivitäten gibt, die der Entwicklung von Hochsicherheitslösungen dienen. Frei zugänglich Hinweise oder Quellen konnten hierfür jedoch nicht identifiziert werden.

Positive Effekte dürften von der in den USA regelmäßig vorzufindenden personellen Verflechtungen zwischen IT-Sektor und öffentlicher Verwaltung sein. Viele der industriellen TC-Akteure sind sowohl für Regierungsorganisation wie etwa die NSA oder NIST tätig gewesen als auch für privatwirtschaftliche Unternehmen oder universitäre Forschungsinstitutionen.

7.2.4 Aktivitäten mit Bezug auf Trusted Computing

7.2.4.1 Nachfrage bei Regierungsorganisationen

Die Verbreitung von TC wird in den USA vor allem durch die Sicherheitsanforderungen im militärischen Umfeld gefördert. Diese Nachfrage dürfte schon in absehbarer Zeit zu einer flächendeckenden Verbreitung von TC-Komponenten, insbesondere TPM, führen.

- Die US-Armee sieht in ihren Planungen für dieses und das kommende Jahr die Ausstattung aller PCs mit TPMs vor.[107]

- Das Department of Defense hat im Sommer 2007 erklärt[108], dass alle neuen Computer wie Server, Desktops, Laptops und PDAs künftig mit einem TPM in der Version 1.2 ausgestattet sein müssen. Ausnahmen sind nur in begründeten Fällen gestattet.

7.2.4.2 Forschungsinstitutionen

Unternehmen wie IBM[109], Microsoft[110] und Intel[111] sind im Bereich der TC-Forschung seit Jahren besonders aktiv. Sie finanzieren Projekte im universitären Umfeld und betreiben eigene Forschung in ihren Labors. Das IBM Global Security Analysis Lab (GSAL) beispielsweise unterwirft TPMs intensiven Konformanztests auf seinen Systemen. Die Ergebnisse der Forschungs- und Testaktivitäten mit TPMs wurden in diversen Whitepapern veröffentlicht. Zudem wurde ein Open Source Treiber für Linux entwickelt und öffentlich verfügbar gemacht.

Das Institute for Security Technology Studies (Dartmouth College) gilt als in den USA führend im Bereich TC. Die Forschungsinstitution arbeitet aktiv in der TCG mit und wird hauptsächlich finanziert vom NIST, der National Cyber Security Division (NCSD), dem

---

107 Department of the Army/Chief Information Officer (2006): 500-Day Plan. Update 2006, Washington.
108 Department of Defense (2007): Memorandum July 3, 2007.
109 "Research for Advancing Trusted Computing": http://domino.research.ibm.com/comm/research.nsf/pages/r.security.innovation.html
110 http://www.microsoft.com/mscorp/twc/iappandrsa/research.mspx.
111 University Research Grant Program sowie Technology and Research: Intel Trusted Execution Technology (http://www.intel.com/technology/security/).

Department of Justice (DOJ), dem Intel University Research Council und dem Ministerium für Nationale Sicherheit, dem Department of Homeland Security. Die Aktivitäten des Institutes sind interdisziplinär angelegt und es werden mit hoher Intensität ökonomische, soziologische und technische Projekte zum Thema TC, Trust sowie Trustworthiness durchgeführt. Das Institut betreibt eigenen Angaben zufolge das maßgebliche PKI Testbed im akademischen Umfeld. Außerdem werden zurzeit als besonders wichtig erachtete Projekte zu Linux und TC durchgeführt. Das Institut arbeitet heute mit finanzieller und personeller Unterstützung von IBM an einem TC Projekt in seinem PKI Research Laboratory.

Die Naval Postgraduate School – Center For Information Systems Security Studies and Research arbeitet ebenfalls an einem maßgeblichen Projekt zur Realisierbarkeit von Trusted Computing. Die Forschungsanstrengungen des „Trusted Computing Exemplar (TCX)" Projektes sollen zeigen, auf welche Weise TC-Systeme und Komponenten sicher und kostengünstig konstruiert werden können und wie sie funktionieren. Ein Projekt zur Entwicklung eines TC-Prototyps wird seit 2003 von dem Office of Naval Research (ONR) und dem National Reconnaissance Office (NRO)[112] finanziert.

7.2.4.3 Unternehmen

Da fast alle wichtigen Unternehmen der US-amerikanischen IT-Wirtschaft in irgendeiner Form in die Entwicklung von TC-Technologien involviert sind, würde es den Rahmen der Studie sprengen, alle Einzelaktivitäten, soweit hierfür Informationen öffentlich zugänglich sind, im Einzelnen vorzustellen. Vor diesem Hintergrund soll nachfolgend auf die wichtigsten Aktivitäten in einzelnen Technologiebereichen bzw. Marktsegmenten fokussiert werden.

Prozessoren / Chipsätze / Grafik

- AMD (Sunnyvale, Kalifornien)

Die AMD Virtualization („Pacifica") Technologie des Chip-Herstellers unterstützt ein Root of Trust for Measurement (RTM). Es bestehen in Deutschland enge Kooperationsbeziehungen zwischen der deutschen Tochtergesellschaft und der Technischen Universität Dresden.

- Intel (Santa Clara, Kalifornien)

Die Trusted Execution Technology (TXT) („LaGrande") Technologie des Chip-Herstellers unterstützt ein Root of Trust for Measurement (RTM). Obwohl Intel seit

---

112 Nationale Aufklärungseinheit, die Satelliten für die jeweiligen Behörden betreibt.

Gründung aktiv in der TCG mitarbeitet, wird nach Experteneinschätzung gleichzeitig an der proprietären Entwicklung von „LaGrande“ festgehalten.

Weitere Produzenten von Chipsätzen und Graphikprozessoren mit TC-Technologie in den USA sind u. a.

- Freescale Semiconductor (Austin, Texas), Ausgliederung von Motorola,
- NVIDIA (Santa Clara, Kalifornien),
- Seagate Technology (Scotts Valley, Kalifornien),
- Texas Instruments (Dallas, Texas).

TPMs / BIOS

Wichtige US-Produzenten im Bereich sind u. a.

- Atmel (San Jose, Kalifornien)

Der Hersteller von integrierten Schaltungen bietet zwei Sicherheitsmodule für Computersysteme und Embedded Systems an, die der TCG Spezifikation 1.2 entsprechen (AT97SC3203, AT97SC3203S).

- Broadcom (San Diego, Kalifornien)

Der Hardwarehersteller für Breitbandanwendungen bietet TPM Hardware-Produkte auf der Basis von Infineon TPM-Technologie an.

- Phoenix (Milpitas, Kalifornien)

Der Softwarehersteller kombiniert BIOS Funktionen und Firmware Sicherheitsprodukte unter Berücksichtigung der TC-Spezifikationen.

- National Semiconductor

Betriebssysteme

- Apple (Cupertino, Kalifornien)

Apple setzt in praktisch allen Produkten TPMs ein[113], deren Funktionalitäten aber nach Firmenangaben derzeit noch nicht durch eine entsprechende Software genutzt werden können.

---

113 Vgl. Lemos, R. (2006), www.securityfocus.com.

- Microsoft (Redmond, Washington)

Das aktuelle Betriebssystem Windows Vista nutzt das TPM mit der Laufwerksverschlüsselung BitLocker, die die Integrität von Windows sicherstellen soll. BitLocker nutzt das TPM 1.2, um Benutzerdaten zu sichern und zu verhindern, dass unerlaubte Änderungen vorgenommen werden, wenn ein Gerät abgeschaltet ist. BitLocker bietet neben der Laufwerksverschlüsselung einen Integritätscheck der frühen Boot-Komponenten, der sicherstellt, dass eine Verschlüsselung nur möglich ist, wenn die Komponenten einer Plattform unverändert erscheinen und das verschlüsselte Laufwerk sich im Original-PC befindet.[114]

Microsoft hat frühzeitig einen Patentschutz für den Einsatz von TC-Technologie im Bereich von Betriebssystemen beantragt. Mindestens seit 2003 verfolgt Microsoft unter dem Entwicklungsnamen „Palladium“, später genannt „Next-Generation Secure Computing Base – NGSCB“ entsprechende Projekte zu TC. Computerexperten haben Microsoft in der Vergangenheit vorgeworfen, mit diesen Projekten nur DRM-Systeme verwirklichen zu wollen, die datenschutzunfreundlich sind und den Anwender entmündigen. Die zurzeit realisierten TC-Komponenten setzen andere Schwerpunkte und sind bei weitem nicht so umfassend wie erwartet.

Im Mai 2007 hat Microsoft die Interoperabilität seiner Network Access Protection Architecture (NAP) mit Trusted Network Connect (TNC) der TCG bekanntgegeben. Diese wird gewährleistet durch eine von Microsoft erarbeitete Spezifikation, die das Unternehmen in die Arbeit der TCG eingebracht hat. Die Spezifikation sorgt dafür, das TNC basierte Produkte mit Windows Clients und Servern interoperabel sind.

Systeme

TPMs werden derzeit bereits von nahezu allen namhaften PC-Herstellern in den Produktreihen für professionelle Anwendungen angeboten. Folgende US-Hersteller bieten inzwischen auch eine softwareseitige Integration bzw. Aktivierung auf ihren Rechnern an:

- Dell (Round Rock, Texas),
- Hewlett-Packard (Palo Alto, Kalifornien),
- IBM (Armonk, New York).

Erste Entwicklungen der heutigen TPM wurden in IBM ThinkPads (Embedded Security Chip / Embedded Security Solution 1.0) eingebaut. IBM bietet außerdem Trusted Server an, die die TNC Spezifikationen unterstützen.

---

114 Vgl. Müller, Th. (2007).

Weitere

Juniper Networks (Sunnyvale, Kalifornien)

Die Unified Access Control (UAC) des Unternehmens fußt auf dem TNC Standard. Juniper Networks und Microsoft streben auf dieser Basis Interoperabilität zwischen Juniper Networks Unified Access Control (UAC) und Microsoft Network Access Protection (NAP) an.

Softex (Austin, Texas)

Softex bietet innerhalb der OmniPass-Produktfamilie und der Produkte Theft Guard TC-basierte Produkte zur Verbesserung der Zugangssicherheit an.

VeriSign (Mountain View, Kalifornien)

Das Security-Unternehmen bietet das Produkt Personal Trust Agent auf der Basis von TC-Spezifikationen an.

Wave Systems (Lee, Massachusetts)

Das Unternehmen bietet das TC-Produkt Embassy Trust Suites an. Die Client- und Serversoftware von Wave Systems wird nach Firmenangaben von allen TPM-Chips unterstützt. Die Software ist z. B. auf vielen Dell-Rechnern vorinstalliert.

7.2.5 Sichtweisen und Kontroversen

Die maßgebliche Verbraucher- und Datenschutzorganisation in den USA, die sich mit Fragen der IT-Sicherheit befasst, ist die Electronic Frontier Foundation (EFF).[115] In dieser Organisation sind international anerkannte Experten tätig. Sie gilt als führend wenn es darum geht, Gesetzesvorlagen begleitend zu kommentieren, mit juristischen Mitteln gegen gesetzliche Regelungen vorzugehen oder die Öffentlichkeit zu mobilisieren. Die EFF hat die kritische Diskussion um TC früh angestoßen und begleitet sie seither konstruktiv mit Änderungsvorschlägen und Kommentaren.

Die EFF hat in der Vergangenheit zwei Whitepaper zum Thema Trusted Computing (2003 und 2004)[116] sowie zahlreiche Kommentare veröffentlicht. Einer der wichtigsten Experten der EFF, Seth Schoen, wurde in den letzten Jahren immer wieder sowohl von den Kritikern als auch von der TC-Entwickler-Community um Stellungnahmen zu be-

---

115 Eine weitere Organisation, die TC wiederholt kritisiert hat, ist die Free Software Foundation von Richard Stallman. Die FSF hat jedoch keine zitierfähigen Whitepaper o.ä. vorgelegt, sondern sich auf Stellungnahmen in den Medien oder bei Veranstaltungen bzw. Anhörungen beschränkt. Die z.T. polemischen Statements werden an dieser Stelle nicht dargestellt.

116 EFF (2003): Trusted Computing: Promise and Risk, October 2003; EFF (2004): Meditations on Trusted Computing, May 2004.

stimmten Entwicklungen gebeten. Er schrieb u. a. auf Aufforderung von in der TCG mitwirkenden Unternehmen einen Kommentar zu Intels „LaGrande Technology Policy on Owner / User Choice and Control“ (Dezember 2003) sowie zu „Trusted Computing Group (TCG)’s Design, Implementation, and Usage Principles” (Oktober 2004).

In einem anderen zentralen Whitepaper “Trusted Computing: Promise and Risk” kritisierten die EFF-Experten das von der TCG verfolgte Prinzip zur Schaffung von hardwarebasierter Sicherheit in aller Schärfe. Insbesondere der Funktionalität der Remote Attestation („Beglaubigung der Plattformkonformität“) wurden erhebliche Auswirkungen in Bezug auf die Privatsphäre der Benutzer zugeschrieben. Da in dem Konzept (später umgesetzt in TPM-Spezifikation Version 1.1) für Remote Attestation eine Trusted Third Party vorgesehen sei, die – so der Verdacht der EFF – Security-Policies entgegen den Wünschen der Nutzer implementieren könne, führe TC zu verpflichtender Rechner-Zugangskontrolle, Einschränkungen der Daten-Kopierbarkeit und Digital Rights Management (DRM), kurz, zum Kontrollverlust des PC-Nutzers über seinen Rechner. Dadurch sei weiterhin zu befürchten, dass TC anti-wettbewerbliche Effekte auf den IT-Markt ausüben werde. Auf Grund einer abnehmenden Interoperabilität bestehe ein wachsendes Risiko von Lock-In-Effekten.[117]

Dieses Problem wurde aus Sicht der EFF nicht dadurch befriedigend gelöst, dass der Nutzer den TPM Chip nicht aktiviert oder in bestimmten Situation das Senden einer Bestätigung unterdrücken kann, wie es im TCG Design vorgesehen ist. Die EFF forderte daher, dass das Merkmal „Owner Override“ zu implementieren sei. Die Vorteile dieses Konzepts sind in der folgenden Tabelle dargestellt.

117 Das Whitepaper von 2004 behandelt ebenfalls dieses Problem, enthält aber keine neuen Aspekte.

Tabelle 7-1: EFF-Vorschlag: Owner Override gewährleistet die Sicherheitsvorteile von Remote Attestation unter Vermeidung der Risiken

	Status quo	**Attestation (TCG)**	**Attestation + Owner Override (EFF)**
Pros	Competition and interoperability are the norm User control and choice are protected Lock-in and remote control are difficult because computer owners have substantial control over all local software in all circumstances	Compromise of software (e.g., by a virus) can be made detectable by a remote party, which can act on this information Cheating in network games can be prevented, and distributed applications (Distributed.net, SETI@Home, etc.) can run on computers owned by untrustworthy parties without risking integrity of calculations or confidentiality of data Organizations can more effectively enforce policies against their own members "Paternalist" security policies that protect users from the consequences of certain of their own mistakes can be implemented	Compromise of software can still be made detectable by a remote party An organization can more effectively enforce policies against its own members, so long as they are using computers owned by the organization Computer owners retain substantial control over local software Competition, interoperability, user control and choice are preserved
Cons	There is no way in general to allow a remote party to detect whether, without the computer owner's knowledge, local software has been inappropriately modified Cheating in network games cannot be prevented Cheating by unscrupulous participants in distributed computing projects cannot be prevented "Paternalist" security policies that protect users against their own mistakes are difficult to enforce	Third parties can enforce policies against computer owner where traditionally these would not have been technologically enforceable, or would have been enforceable only with difficulty -- for example: • DRM • application lock-in • migration and back-up restrictions • product activation • product tethering • forced upgrade • forced downgrade • application-specific spyware • preventing reverse engineering, etc.	Cheating in network games or by unscrupulous distributed computing participants still cannot be prevented "Paternalist" security policies remain difficult to enforce To the extent that computer owners might potentially benefit from the robust enforcement of DRM policies, they would not obtain those benefits

Quelle: EFF (2004)

Nicht zuletzt auf Grund der nicht nur von der EFF, sondern auch in von vielen ausländischen Organisationen und Einzelpersonen vorgetragenen Kritik veränderte die TCG die entsprechende Funktionalität. Mit der TPM-Spezifikation Version 1.2 wurde von der TCG ein als Direct Anonymous Attestation (DAA) bezeichnetes Verfahren eingeführt. Über das kryptographische Signaturschema des Zero Knowledge können seither Verifikationen vorgenommen werden, ohne dass eine Trusted Third Party eingeschaltet werden muss.

Dieses Verfahren und die Berücksichtigung weiterer Kritikpunkte wurde von Daten- und Verbraucherschützern explizit begrüßt. Die konstruktive Haltung der TCG führte dazu, dass Trusted Computing auch innerhalb der EFF als „rotes Tuch ausgedient“[118] hat. Der konstruktive Dialog zwischen EFF-Experten und TCG-Industrievertretern wird von beiden Seiten als erfolgreich in Bezug auf die Umsetzung der Datenschutzerfordernisse gewertet. Aus EFF-Sicht aber bleibt die Forderungen aktuell, dass jedes Endgerät auch bei Implementierung von TC-Funktionalitäten den Prinzipien von Offenheit, Flexibilität und Programmierbarkeit folgen muss. Diese Prinzipien sind es schließlich, die in der Vergangenheit zu seiner breiten Diffusion in geschäftlichen und privaten Anwendungskontexten sowie zu seinem Innovationspotential entscheidend beigetragen haben.

Insgesamt beschränkt sich die Dokumentation der TC-Diskussion auf der EFF Website auf Veröffentlichungen aus den Jahren 2003 bis 2005.[119] Etwa ab Beginn des Jahres 2006 werden aus Sicht der EFF weitreichende Verständigungsfortschritte mit der TCG erzielt. Da die EFF im den Bereichen Konsumentenschutz, Datenschutz sowie Privacy in den USA eine Art Meinungsführerschaft besitzt, hat ihre konstruktive Haltung erheblichen Einfluss auf die Versachlichung der öffentlichen Debatte genommen. So ist es nicht verwunderlich, dass grundsätzliche Kritiken an den von der TCG verfolgten Standardisierungsaktivitäten seither nicht mehr vorgebracht wurden bzw. keine entsprechenden Hinweise gefunden werden können.

7.2.6 Zwischenfazit

- Seit Ende 2005 sind die Kritiker der TCG-Standards in den USA weitgehend verstummt. Die neuen Spezifikationen (insbesondere der Standard 1.2) gelten seither auch unter Verbraucher- und Datenschutzakteuren als hinreichend dafür, dass die Belange des Datenschutzes, der Verfügungshoheit sowie der Privatsphäre bei TC berücksichtigt werden.

---

118 Computerzeitung v. 31.10.2006 „Trusted Computing hat als rotes Tuch ausgedient“.

119 Why Would MS Do Hollywood's Bidding? August 12, 2005; Your General-Purpose PC - Hollywood-Approved Entertainment Appliance, August 09, 2005; Microsoft Sells Out the Public on CGMS-A, July 27, 2005; Protected Media Path, Component Revocation, Windows Driver Lockdown, July 25, 2005; The Dangers of Device Authentication, July 19, 2005; Microsoft Trusted Computing Updates, July 15, 2005.

- Die führenden US-amerikanischen IT-Unternehmen sind bei der Entwicklung und Verbreitung von Trusted Computing dominierend. Ihre Innovationskraft wirkt – nicht zuletzt über ihre aktive Mitarbeit in der TCG - weltweit als Treiber für diesen neuen Sicherheitsstandard. Zurzeit gibt es keine Hinweise darauf, dass der Einsatz von TC-Komponenten in den Produkten von US-IT-Herstellern zu einer Verschärfung von Interoperabilitätsproblemen oder anderen, wettberbsbehindernden Lock-In-Effekten geführt hat. Eine solche Einschätzung kann erst vorgenommen werden, wenn TC-Funktionalitäten zunehmen aktiv genutzt werden und über die gesamte IT-Wertschöpfungskette TC zum Einsatz kommen. Davon ist der US-Markt nach Einschätzung der Experten jedoch noch ein paar Jahre entfernt.

- Im Gegensatz zu China ist der Einfluss des öffentlichen Sektors in den USA weitaus weniger greifbar. Das Verhältnis zu TC kann als pragmatisch und weniger als strategisch beschrieben werden. Zum einen sorgt die Beschaffungsstrategie der öffentlichen Hände mit dem klaren Fokus auf COTS-Produkten dafür, dass bei Bedarf auf Massenmarkt-Produkte zurückgegriffen wird und auch werden kann. Die Untersuchung zeigt, dass fast alle großen und wichtigen Hersteller inzwischen TC-Funktionalitäten in ihre Produkte integrieren. Zum anderen gibt es zahlreiche Hinweise, dass in vielen Firmenlabors sowie auch in Universitäten in erheblichem Umfang TC-relevante F&E-Aktivitäten vorangetrieben werden, so dass der Einsatz öffentlicher Mittel sich auf die Hochsicherheitsrelevanten Bereiche beschränken kann. Es kann jedoch davon ausgegangen werden, dass sowohl das US-Militär als auch die nationalen Sicherheitsbehörden (NSA, NIST) im Bereich TC aktiv sind.

- Sicherheitssensitive Regierungseinheiten wie das Verteidigungsministerium und die US-Army profitieren von den neuen Technologien und fördern ihren zivilen Einsatz indirekt durch ihre massive Nachfrage. Ohne Zweifel spielt TC in der Sicherheitsstrategie der USA eine sehr wichtige Rolle. Das Militär übernimmt die Rolle des frühen Anwenders und sorgt auf diese Weise für die Verbreitung von TC. Die mit diesem Bereich zusammenarbeitenden Industriebranchen werden rasch folgen. Weitere geschäftliche Nutzer werden auf Grund von Kompatiblitäts- und Interoperabilitätsüberlegungen folgen.

- Das Industriekonsortium TCG hat bereits zahlreiche Innovationen bei IT-Hard- und Softwareherstellern angestoßen. Sowohl universitäre als auch privatwirtschaftliche Forschungsinstitutionen betreiben F&E auf dem Gebiet des Trusted Computing. Dies legt nahe, dass auf der Basis der neuen Standards in absehbarer Zeit weitere innovative Anwendungen entwickelt werden. Die in den USA angesiedelten Unternehmen decken die gesamte IT-Wertschöpfungskette ab und verfolgen somit faktisch eine TC-Gesamtstrategie, deren Koordination scheinbar alleine über Marktmechanismen erfolgt. Eine industriepolitische Koordination oder Förderung durch den Staat wird offenkundig als nicht notwendig erachtet.

- Die Verbreitung von TPM wird zurzeit von pragmatischen Erwägungen getrieben. Die entsprechenden Prozessoren werden in die Hardware integriert, ob sie bereits von Anwendungen benötigt werden, spielt noch keine Rolle. Zum jetzigen Zeitpunkt erscheint unklar, wie TC Technologie konkret flächendeckend eingesetzt werden wird. Manche grundsätzlichen Fragen nach der Funktionabilität und Interoperabilität im Massenmarkt sowie der faktischen Sicherheit von TC Anwendungen sind auch in den USA noch nicht beantwortet.

- Da sowohl in der öffentlichen Verwaltung, in der Politik sowie bei Produzenten und privaten bzw. geschäftlichen Nachfragern nunmehr Konsens darüber herrscht, dass TC eine wichtige Funktionalität für die gesamte IT-Landschaft darstellt, wird mit einer raschen Verbreitung gerechnet.

8 Wettbewerbspolitische Implikationen

Funktionsfähiger Wettbewerb wirkt wohlfahrtsoptimierend.[120] Gerade in Märkten, die wie die IT-Märkte durch Netzexternalitäten[121], Größen-[122] und Verbundvorteile[123] sowie vertikale Integration[124] geprägt sind, sieht sich der Wettbewerbsprozess jedoch erheblichen Gefahren ausgesetzt: Solche Märkte weisen eine besondere Tendenz zur Konzentration wirtschaftlicher Macht auf.[125] Außerdem kommt es zu Pfadabhängigkeiten[126], durch welche die Wechselbereitschaft und -fähigkeit der Verbraucher beschränkt wird; zugleich haben Unternehmen, die sowohl auf vor- als auch auf nachgelagerten Märkten tätig sind, erhebliche Diskriminierungsanreize und -möglichkeiten. Angesprochen sind somit die drei primären wettbewerblichen Fehlentwicklungen, deren Unterbindung das allgemeine Wettbewerbsrecht zum Ziel hat, nämlich die Behinderung von Wettbewerbern sowie die Ausbeutung und Diskriminierung von Wettbewerbern und Verbrauchern.

Die auf IT-Märkten generell zu gewärtigenden wettbewerbspolitischen Gefahren wurden auch schon früh für den Wettbewerb um „Trusted Computing"-Plattformen und um komplementäre Produkte und Dienstleistungen gesehen.[127] Im Rahmen des nachfolgenden Kapitels soll untersucht werden, inwieweit diese theoretische Gefahrenprognose mit tatsächlichen Risiken für die Bewegungsfreiheit der unsichtbaren Hand des Wettbewerbs einhergeht (dazu unter 8.1) und welche Auswirkungen auf die relevanten Märkte hiervon potentiell ausgehen (dazu unter 8.2). Hierauf aufbauend sind schließlich potentielle Reaktionsmöglichkeiten darzustellen und zu analysieren (dazu unter 8.3).

Dabei wird der Schwerpunkt durchweg auf das europäische und das (ihm seit der 7. GWB-Novelle mittlerweile weitgehend nachgebildete) deutsche Wettbewerbsrecht gelegt, während namentlich das Wettbewerbsrecht der Vereinigten Staaten von Ameri-

---

120 Koenig/Vogelsang/Kühling/Loetz/Neumann, Funktionsfähiger Wettbewerb auf den Telekommunikationsmärkten, 2002, S. 26 f.

121 Von einer Netzexternalität spricht man dann, wenn die Nutzung eines Produktes durch einen zusätzlichen Nachfrager Auswirkungen auf den Wert der Nutzung des Produktes durch die bestehenden Nutzer – den sog. „installierten Bestand" („installed base") – hat, vgl. Koenig/Loetz/Neumann, Telekommunikationsrecht, 2004, S. 42; Koenig/Vogelsang et al. (Fn. 120), S. 90; siehe auch Heinemann, CR 2005, 715, 716.

122 Hiervon spricht man, wenn mit wachsender Produktionsmenge die Durchschnittskosten sinken, vgl. Heinemann, CR 2005, 715, 716; Koenig/Loetz/Neumann (Fn. 121), S. 43.

123 Ein Verbundvorteil tritt auf, wenn die Produktion mehrerer Güter durch ein Unternehmen gegenüber der Produktion der einzelnen Güter durch unterschiedliche Unternehmen Kostenvorteile mit sich bringt, Koenig/Loetz/Neumann (Fn. 121), S. 43 f.

124 Vertikale Integration liegt vor, wenn ein Unternehmen auf unterschiedlichen Produktionsstufen (im Sinne vor- und nachgelagerter Märkte) tätig ist, Koenig/Loetz/Neumann (Fn. 121), S. 45.

125 Heinemann, CR 2005, 715, 716.

126 Von einer Pfadabhängigkeit spricht man, wenn eine Kaufentscheidung auf Grund getätigter Investitionen und hoher Wechselkosten nachfolgende Kaufentscheidungen beeinflusst.

127 Bechtold, in: Koenig/Neumann/Katzschmann, Trusted Computing, 2004, S. 77, 88 ff.; Bechtold, CR 2005, 393, 396 ff.; Koenig/Neumann, in: Koenig/Neumann/Katzschmann, a. a. O., S. 100; Koenig/Neumann, DuD 2004, 555 Koenig/O'Sullivan, ECLR 2003, 449; Neumann, in: Taeger/Wiebe, Mobilität Telematik Recht, 2005, S. 187, 210 ff. Vgl. auch Blaha, Trusted Computing auf dem Prüfstand des kartellrechtlichen Missbrauchsverbotes, 2006.

ka wegen seiner erheblichen strukturellen Unterschiede trotz praktisch ähnlicher Anwendungsergebnisse[128] nur bedingt vergleichbar ist. Außer Betracht bleiben auch die wettbewerbspolitischen Risiken von Unternehmenszusammenschlüssen in IT-Märkten.[129] Diese Risiken sind allgemeiner Natur und nicht spezifisch für den Bereich des „Trusted Computing".

8.1 Risiken

Hinsichtlich des Bestehens von Risiken für einen wohlfahrtsoptimierenden Wettbewerbsprozess sind auch im Falle von „Trusted Computing" zunächst die Erkenntnisse von zumindest potentieller Bedeutung, die sich allgemein auf die Existenz entsprechender Gefahren in IT-Märkten beziehen (dazu unter 8.1.1). Diese lassen sich dann in einem zweiten Schritt mit Blick auf die besonderen Verhältnisse der „Trusted Computing"-Märkte konkretisieren (dazu unter 8.1.2).

8.1.1 Analyse der relevanten Wettbewerbsrisiken in IT-Märkten

Eine Analyse der Wettbewerbsrisiken, die allgemein in IT-Märkten bestehen und deshalb auch für die „Trusted Computing"-Märkte von Bedeutung sein können, muss auf der wettbewerbsrechtlichen Entscheidungspraxis der Behörden und Gerichte und auf den Erkenntnissen der theoretischen Literatur aufbauen.

8.1.1.1 Wettwerbsrechtliche Entscheidungspraxis

Bei der Auswertung der wettbewerbsrechtlichen Entscheidungspraxis geht es alleine um die praktischen Erfahrungen mit der Anwendung des Wettbewerbsrechts in den eigentlichen IT-Märkten, nicht jedoch in lediglich *IT-gestützten* Märkten, wie beispielsweise im Bereich der Internetplattformen[130]. Diese Marktebene ist den hier interessierenden Hardware- und Software-Märkten nachgelagert und weist eigenständige spezifische Probleme auf, deren Einbeziehung die Ergebnisse der nachfolgenden Analyse von dem eigentlichen Gegenstand der Untersuchung entfernen würde.

---

128 Vgl. Möschel, ZWeR 2007, 261, 263.
129 Siehe hierzu etwa BKartA, Beschl. v. 23.12.2005 – Az. B 7 – 162/05, WuW/E DE-V 1221; Beschl. v. 4.1.2000 – Az. B 7 – 225/99, WuW/E DE-V 328; Heinemann, CR 2005, 715, 718.
130 Siehe dazu etwa Heinemann, CR 2005, 715, 719.

8.1.1.1.1 Deutsches Wettbewerbsrecht

Eine Analyse der Entscheidungspraxis der deutschen Wettbewerbsbehörden und -gerichte fördert allerdings kaum Beispiele für die Anwendung des Wettbewerbsrechts in den vorstehend eingegrenzten IT-Märkten zutage.

Die Tätigkeitsberichte des Bundeskartellamtes berichten aus diesem Bereich fast ausschließlich von Zusammenschlussverfahren.[131] Nur in ganz wenigen Fällen ging es um (andere) Verhaltensvorgaben des Wettbewerbsrechts. Dabei betraf ein Fall mit der Anwendung der Buchpreisbindung auf CD-ROM-Erzeugnisse eine im vorliegenden Kontext irrelevante Sondervorschrift.[132] Die verbleibenden Verfahren, die auf die Anwendung der wettbewerbsrechtlichen Kernnormen gerichtet waren, bezogen sich ausschließlich auf die Ebene des Vertriebs fertiger Produkte.[133] Die entsprechenden Verfahren wurden eingestellt, zumeist nach einer Abmahnung durch das Bundeskartellamt, die zu einer Änderung des beanstandeten Verhaltens führte,[134] aber auch wegen zwischenzeitlich ergangener Rechtsprechung des BGH[135] zu zivilrechtlichen Vorfragen[136].

In der damit angesprochenen Rechtsprechung der deutschen (Zivil-) Gerichte finden sich ebenfalls nur wenige Fälle, in denen es um die Anwendung des hier relevanten Wettbewerbsrechts[137] in den typischen IT-Märkten[138] geht. Zu nennen sind hier insbesondere die Urteile, die vor der vorgenannten BGH-Entscheidung von den Instanzgerichten gefällt wurden. Diese hatten in der Bindung eines Softwareverkaufs an den gleichzeitigen Verkauf von Hardware keinen Verstoß gegen das wettbewerbsrechtliche

---

131 Siehe etwa BKartA, Tätigkeitsbericht 2005/2006, BT-Drs. 16/5710, 163 f.; Tätigkeitsbricht 2003/2004, BT-Drs. 15/5790, 118 f. u. 173; Tätigkeitsbericht 2001/2002, BT-Drs. 15/1226, 213 ff.; Tätigkeitsbericht 1999/2000, BT-Drs. 14/6300, 119, 121 u. 171 f.; Tätigkeitsbericht 1997/1998, BT-Drs. 14/1139, 160 f.; Tätigkeitsbericht 1995/1996, BT-Drs. 13/7900, 149 ff.

132 BKartA, Tätigkeitsbericht 1995/1996, BT-Drs. 13/7900, 150 f.

133 BKartA, Tätigkeitsbericht 2001/2002, BT-Drs. 15/1226, 214 (angenommene vertragliche Wettbewerbsbeschränkung in Verträgen zwischen Sony und „Playstation"-Zwischenhändlern); Tätigkeitsbericht 1999/2000, BT-Drs. 14/6300, 170 (angenommene Diskriminierung eines Zwischenhändlers durch Sony beim „Playstation"-Vertrieb) u. 170 f. (angenommene Behinderung und Diskriminierung gegenüber kleinen Softwarehändlern durch Microsoft beim Vetrieb sog. OEM-Versionen [Original Equipment Manufacturer]).

134 BKartA, Tätigkeitsbericht 2001/2002, BT-Drs. 15/1226, 214; Tätigkeitsbericht 1999/2000, BT-Drs. 14/6300, 170.

135 BGH, Urt. v. 6.7.2000 – Az. I ZR 244/97, BGHZ 145, 7.

136 BKartA, Tätigkeitsbericht 1999/2000, BT-Drs. 14/6300, 171.

137 Auch in der Rechtsprechung kommen neben Zusammenschlussverfahren im vorliegenden Kontext irrelevante Sondervorschriften des Wettbewerbsrechts zur Anwendung, namentlich auch die Buchpreisbindung, vgl. BGH, Beschl. v. 11.3.1997 – Az. KVR 39/95, BGHZ 135, 74; KG, Beschl. v. 17.5.1995 – Az. Kart 14/99, WRP 1995, 938.

138 Den Internetbereich betrifft demgegenüber die Entscheidung des OLG Frankfurt a. M., Urt. v. 23.11.1999 – Az. 11 U (Kart) 1/99, MMR 2000, 559 (keine unzulässige Behinderung oder Diskriminierung des Anbieters einer providerfremden Suchmaschine durch T-Online, wenn dessen Suchmaschine auf der Einstiegsseite von T-Online anders als die providereigene Suchmaschine nur über mehrere Zwischenschritte erreichbar ist).

Kartellverbot gesehen,[139] betrafen also – wie vereinzelte Urteile anderer (Zivil-) Gerichte[140] – auch nur die Ebene des Produktvertriebs.

Besonders hervorzuheben ist allerdings, dass unlängst in einigen Gerichtsentscheidungen die Frage der Diskriminierung und des Ausbeutungsmissbrauchs im Zusammenhang mit Lizenzverträgen zur Nutzung des MPEG 2-Standards aufgeworfen wurde.[141] Im wettbewerbsrechtlichen Kern ging es bei diesen Verfahren im Grenzbereich zwischen IT und Unterhaltungselektronik um die Frage, ob die angebotenen Lizenzvereinbarungen angemessen und diskriminierungsfrei waren, oder ob hier Lizenzgebühren für Schutzrechte verlangt wurden, die aus technischen Gründen eigentlich nicht benötigt würden.

Das Gericht wies die entsprechenden Vorwürfe zurück, da die Partei, die sich auf die Wettbewerbsrechtswidrigkeit des Standardisierungs- und Lizenzierungsverhaltens berufen hatte, die hierfür notwendigen substantiierten Darlegungen und Nachweise schuldig geblieben war. Dass der betroffene Standard-Lizenzvertrag als Vergütung eine feste Stücklizenzgebühr und keinen prozentualen Anteil am Fabrikabgabepreis vorsieht, hielt das Gericht darüber hinaus für (wettbewerbs-) rechtlich unbedenklich. Die erstinstanzlichen Gerichtsverfahren dauerten z. T. weniger als anderthalb Jahre.[142] Sie sind aber Bestandteil einer Serie von Patentprozessen, die schon seit sechs Jahren die Gerichte beschäftigen, die aber zumeist mit einer außergerichtlichen Lösung enden.[143]

8.1.1.1.2 EG-Wettbewerbsrecht

Bei der Anwendung des EG-Wettbewerbsrechts durch die Kommission im Bereich der IT-Märkte hat diese ausweislich der jährlichen Berichte über die Wettbewerbspolitik bereits eine Vielzahl von Missbrauchs- und Kartellverfahren im IT-Bereich durchgeführt.[144] Dabei hat die Kommission einige Verfahren eingestellt, weil sich die behauptete Wettbewerbsbeschränkung nicht feststellen ließ. Grund hierfür war u. a., dass die

---

139 LG Berlin, Urt. v. 27.8.1996 – Az. 16 O 581/95, CR 1996, 730 (nachgehend: KG, Urt. v. 17.6.1997 – Az. 5 U 7145/96, CR 1998, 137). Siehe entsprechend auch in einem Parallelverfahren KG, Urt. v. 27.2.1996 – Az. 5 U 8281/95, NJW 1997, 330. Der BGH hat die vorinstanzlichen Entscheidungen aufgehoben, brauchte sich dabei aber nicht mit der wettbewerbsrechtlichen Bewertung einer entsprechenden Vertriebsbeschränkung zu befassen, BGH, Urt. v. 6.7.2000 – Az. I ZR 244/97, BGHZ 145, 7.

140 OLG München, Urt. v. 24.2.1994 – Az. U (K) 3669/93; Urt. v. 30.3.1990 – Az. 7 U 2469/90, CR 1991, 731.

141 Vgl. beispielhaft für mehr als ein Dutzend Parallelverfahren LG Düsseldorf, Urt. v. 30.11.2006 – Az. 4b O 346/05, Rn. 127 ff. (Juris). Instruktiv zu der Problematik Ullrich, GRUR 2007, 817.

142 Im Verfahren LG Düsseldorf, Urt. v. 30.11.2006 – Az. 4b O 346/05, war unter dem 14.7.2005 Klage erhoben worden.

143 Siehe hierzu die Juve-Nachricht v. 29.3.2007 („ODS verletzt Patente des MPEG2-Pools)".

144 Von aktuellem Interesse ist das gegen den Chiphersteller Qualcomm im Oktober 2007 eingeleitete Verfahren; hier sieht die Kommission Anhaltspunkte für die missbräuchliche Ausübung von Marktmacht durch die Ausgestaltung von Lizenzbedingungen (einschließlich der Lizenzentgelte).

betreffenden Beschwerdeführer kein hinreichendes Beweismaterial vorlegen konnten.[145]

Zumeist konnten die Verfahren, die von der Kommission in IT-Märkten eingeleitet worden waren, aber ohne förmliche Entscheidung zu einem Abschluss gebracht werden, da das beanstandete Verhalten nach entsprechender Intervention der Kommission abgestellt wurde. Dies betraf u. a. Fälle vertraglicher Wettbewerbsbeschränkungen, mit denen der Wettbewerb auf nachgelagerten IT-Märkten beschränkt wurde,[146] aber auch die Drohung mit der Nichtbelieferung von Händlern im Falle eines Vertriebes von Konkurrenzprodukten[147] und die missbräuchliche Ausgestaltung von Lizenzbestimmungen gegenüber Wettbewerbern auf nachgelagerten IT-Märkten[148].

Zu dieser Gruppe von Verfahren, die nach einer Anpassung des Verhaltens eingestellt wurden, gehört auch das Verfahren gegen IBM aus dem Jahr 1984.[149] In diesem Verfahren sah die Kommission in insgesamt vier Verhaltensweisen einen Marktmachtmissbrauch: in der nicht rechtzeitigen Mitteilung von Schnittstelleninformationen an Wettbewerber auf nachgelagerten Märkten, in der Kopplung von Hauptprozessoren (Central Processing Units, CPU) mit Speicherbausteinen einerseits und der Betriebssystemsoftware andererseits sowie in der Weigerung, Nutzern anderer Hauptprozessoren bestimmte Softwareinstallationsdienste zur Verfügung zu stellen. Dieses Verfahren erstreckte sich über insgesamt vier Jahre, wobei sich IBM erst unmittelbar vor Erlass einer förmlichen Verbotsentscheidung und nach mehreren Verhandlungsrunden zur Änderung des beanstandeten Verhaltens bereiterklärte.

Von gewisser Prominenz ist des Weiteren das Verfahren in der Sache X/Open Group aus dem Jahr 1986, in dem es um die Entwicklung einer offenen Industrienorm für eine gemeinsame Unix-Anwendungsumgebung ging.[150] Die Kommission stellte fest, dass die Mitgliedschaft in einer Organisation, die einen marktrelevanten Standard[151] entwi-

---

145 Kommission, Bericht über die Wettbewerbspolitik 2000, S. 173 f. (angeblich unfaire Lizenzvereinbarungen von Microsoft gegenüber OEM-Herstellern).

146 Kommission, Bericht über die Wettbewerbspolitik 1999, S. 183 (als wettbewerbsbeschränkend erachtete Vertragsklauseln bei der Vergaben von Lizenzen für den „Internet Explorer“ durch Microsoft); Bericht über die Wettbewerbspolitik 1998, S. 175 f. (angenommene Wettbewerbsbeschränkung durch vertragliche Vereinbarung eines Genehmigungsvorbehaltes für Videospiele unabhängiger Hersteller zugunsten von Sony); Bericht über die Wettbewerbspolitik 1997, Rn. 79 (S. 33) (potentiell wettbewerbsbeschränkende Verpflichtung der Santa Cruz Operation Inc., die Kompatibilität zu veralteten Programme ihres Wettbewerbers Microsoft zu wahren) u. Rn. 80 (S. 33 f.) (angenommene Wettbewerbsbeschränkung durch vertragliche Vereinbarung eines Genehmigungsvorbehaltes für Videospiele unabhängiger Hersteller zugunsten von Sega und Nintendo).

147 Kommission, Bericht über die Wettbewerbspolitik 2002, S. 228 (angebliche Behinderung des Firewall/VPN-Herstellers Stonesoft durch CheckPoint).

148 Kommission, Bericht über die Wettbewerbspolitik 2002, S. 228 f. (angenommener Marktmachtmissbrauch von IBM gegenüber AllVoice durch Klageverbot und Wertschöpfungsverpflichtung).

149 Zu diesem Verfahren etwa Heinemann, CR 2005, 715, 716; Lomholt, Competition Policy Newsletter 3/1998, 7.

150 Entscheidung der Kommission v. 15.12.1986 – Az. IV/31.458, ABl. EG 1987 L 35, 36 – X/Open Group.

151 Die Kommission stellte maßgeblich darauf ab, dass Softwarehersteller an der Einhaltung dieses Standards sehr interessiert sein würden.

ckelt, ihren Mitgliedern einen spürbaren Wettbewerbsvorsprung gegenüber ihren Wettbewerbern verschaffen kann, namentlich angesichts der besonderen Bedeutung zeitlicher Vorsprünge in den dynamischen IT-Märkten. Die Kommission ging davon aus, dass unter diesen Voraussetzungen eine grundsätzlich unzulässige Wettbewerbsbeschränkung nur dann nicht vorliege, wenn die Mitgliedschaft allen beteiligungswilligen Unternehmen zu diskriminierungsfreien Bedingungen offenstehe. Obwohl die Kommission diese Voraussetzungen in dem damaligen Fall als nicht erfüllt ansah, verbot sie die Standardisierungsinitiative nicht wegen eines Verstoßes gegen das Kartellverbot, weil sie davon ausging, dass die Wettbewerbsbeschränkungen durch damit einhergehende Vorteile für die Verbraucher ausnahmsweise gerechtfertigt seien. Sie stellte die Initiative daher ein halbes Jahr nach Verfahrenseinleitung vom Kartellverbot frei.

Nicht alle wettbewerbsrechtlichen Verfahren der Kommission im IT-Bereich endeten jedoch ohne eine abschließende Verbotsentscheidung der Kommission. So hat diese u. a. nach Abschluss eines etwa zwei Jahre dauernden Verfahrens Vereinbarungen untersagt, mit denen der Parallelhandel mit Spielkonsolen und –kassetten beschränkt worden war.[152] Bislang wohl am aufsehenerregendsten war aber die „Microsoft“-Entscheidung der Kommission aus dem Jahr 2004.[153]

Dieser Entscheidung waren fünfjährige Ermittlungen vorausgegangen. Im Ergebnis stellte die Kommission fest, dass Microsoft durch die Nichtoffenlegung bestimmter Schnittstelleninformationen seine beherrschende Stellung auf dem Markt für Arbeitsgruppenserver missbraucht habe. Daneben habe Microsoft seine Marktmacht auch auf dem Markt für PC-Betriebssysteme missbraucht, indem es den Erwerb des „Windows“-Betriebssystems vom gleichzeitigen Erwerb des „Windows Media Player“ abhängig gemacht habe.

Als Abhilfemaßnahmen wurde die Offenlegung und künftige Aktualisierung der vollständigen und genauen Schnittstellenspezifikationen angeordnet, deren Nutzung überdies zu vernünftigen und nicht diskriminierenden Bedingungen erlaubt werden müsse. Außerdem wurde Microsoft verpflichtet, eine voll funktionsfähige „Windows“-Version ohne integrierten „Windows Media Player“ anzubieten. Zur Überwachung dieser Verhaltensmaßgaben sollte auf Kosten von Microsoft ein Bevollmächtigter eingesetzt werden, dem Microsoft umfassenden Zugang zu den benötigten Informationen einräumen müsse. Außerdem wurde eine Geldbuße in Höhe von 492,2 Mio. Euro verhängt.

Gegen diese Entscheidung hat Microsoft vor dem EuG geklagt und kurz darauf einen Antrag auf Aussetzung des Vollzugs nach Art. 242 EG i. V. m. Art. 225 Abs. 1 EG ge-

---

152 Kommission, Bericht über die Wettbewerbspolitik 2000, S. 207 f. (= Entscheidung der Kommission v. 30.10.2002 – Az. COMP/35.587, 35.706 u. 36.321, ABl. EU 2003 L 255, 33).

153 Kommission, Entscheiung v. 24.3.2004 – Az. COMP/C-3/37.792 – Microsoft, deutschsprachige Zusammenfassung abgedruckt in ABl. EU 2007 L 32, 23. Zu dieser Entscheidung etwa Heinemann, CR 2005, 715, 717.

stellt. Dieser Antrag wurde vom Präsidenten des EuG noch im Jahr 2004 abgelehnt.[154] Maßgeblich hierfür war in erster Linie die Bewertung, dass sich die Aussetzung des Vollzugs bis zur Entscheidung in der Hauptsache nicht als dringlich[155] darstellte.[156] Die materiell-rechtlichen Kernfragen beantwortete das EuG dann erst in seinem Urteil, das am 17. September 2007 verkündet wurde.[157] Hierin bestätigte es weitgehend die Entscheidung der Kommission, die es nur hinsichtlich der Einsetzung eines Überwachungsbevollmächtigten aufhob. Für eine solche Abhilfemaßnahme vermochte das EuG keine Grundlage im Gemeinschaftsrecht zu erkennen.

8.1.1.1.3 Analyse der Entscheidungspraxis

Eine Analyse der deutschen und europäischen Entscheidungspraxis zeigt, dass spezifische Aspekte der IT-Märkte bislang nur gelegentlich Gegenstand wettbewerbsrechtlicher Verfahren waren. Dabei liegt zumindest bislang der Schwerpunkt dieser Verfahrenpraxis auf europäischer Ebene, während sich die deutschen Wettbewerbsbehörden und Gerichte nur selten mit Gefahren für den Wettbewerb in IT-Märkten befassen mussten.

Generell ist festzustellen, dass die Mehrzahl entsprechender Verfahren der deutschen und europäischen Wettbewerbsbehörden ohne förmliche Feststellung eines Wettbewerbsverstoßes und einer daran anknüpfenden Verbotsentscheidung abgeschlossen wurde. Vielmehr wurde das beanstandete Verhalten in aller Regel geändert, nachdem die betreffende Wettbewerbsbehörde ihre diesbezüglichen Bedenken mitgeteilt hatte. In einigen Fällen wurden Verfahren auch deshalb eingestellt, weil die dortigen Beschwerdeführer den behaupteten Wettbewerbsverstoß nicht hinreichend substantiiert darlegen und nachweisen konnten. Das gilt gerade auch für die seltenen Fälle, in denen die Einhaltung des Wettbewerbsrechts in IT-Märkten zwischen zwei Unternehmen vor Gericht umstritten war.

Hinsichtlich der auftretenden Gefahren für den Wettbewerb auf IT-Märkten sind zwar einige Fälle bekannt, in denen versucht wurde, den Vertrieb von IT-Erzeugnissen entweder durch einseitige Maßnahmen oder kollusiv zu beschränken. Solche Vorgehensweisen sind aber kein Spezifikum von IT-Märkten, sondern in allen Wirtschaftsbereichen mit mehrstufigen Wertschöpfungsketten anzutreffen. Mit Blick auf die wettbewerbsrechtlichen Anforderungen an die Standardisierung in den dynamischen IT-

---

154 EuG, Beschl. v. 22.12.2004 – Rs. T−201/04 R.

155 Nach ständiger Rechtsprechung ist die Frage der Dringlichkeit des Erlasses einer einstweiligen Anordnung danach zu beurteilen, ob die Gewährung vorläufigen Rechtsschutzes erforderlich ist, um zu verhindern, dass dem Antragsteller ein schwerer und nicht wieder gutzumachender Schaden entsteht, EuG, Beschl. v. 22.12.2004 – Rs. T−201/04 R, Rn. 240 u. 416 m. w. N.

156 EuG, Beschl. v. 22.12.2004 – Rs. T−201/04 R, Rn. 226 ff. u. 405 ff.

157 EuG, Urt. v. 17.9.2007 – Rs. T-201/04.

Märkten hat die Kommission schon früh das aus dem Kartellverbot abgeleitete Erfordernis einer offenen Mitgliedschaft zu diskriminierungsfreien Bedingungen betont.

Typische Wettbewerbsgefahren ergeben sich in IT-Märkten ausweislich der vorgefundenen Verfahrenspraxis auch durch die Notwendigkeit, Rechte zur Nutzung gewerblicher Schutzrechte in Lizenzen zu erwerben. Hier bestehen ersichtliche Möglichkeiten und Anreize, durch entsprechende Lizenzklauseln oder -vereinbarungen den Wettbewerb auf den nachgelagerten IT-Märkten entweder einseitig oder kollusiv zu beschränken.

Mit Blick auf die einseitige Ausübung von Marktmacht in wettbewerbswidriger Weise wurden in der wegweisenden Microsoft-Entscheidung der Kommission zwei wettbewerbswidrige Verhaltensweisen identifiziert: die Nichtoffenlegung bestimmter Schnittstelleninformationen gegenüber Wettbewerbern auf nachgelagerten Märkten und die Verknüpfung eines marktdominanten Plattformproduktes mit einem Produkt, das einem nachgelagerten Wettbewerbsmarkt zuzuordnen ist. Die Microsoft-Entscheidung ist aber auch mit Blick auf die zeitliche Dimension entsprechender Verfahren von Interesse: Die vorhergehenden Ermittlungen hatten fünf Jahre gedauert, die gerichtliche Überprüfung der Entscheidung (durch das erstinstanzlich zuständige EuG) nahm weitere drei Jahre in Anspruch.

8.1.1.2 Wettwerbsrechtliche Literatur

Angesichts der überschaubaren Entscheidungspraxis sind die Erkenntnisse der wettbewerbsrechtlichen Literatur[158] für eine Analyse der Wettbewerbsrisiken in den IT-Märkten von besonderem Gewicht. Dabei erscheint mit Blick auf eine wettbewerbspolitische Auseinandersetzung eine szenarienorientierte Betrachtungsweise besonders ergiebig, bei welcher der Blick auf die zu bewertenden Verhaltensweisen gerichtet wird:

- Wettbewerbsbeschränkung durch Standardisierung
    - Eine verbindliche Verpflichtung zur Einhaltung eines Standards wird in aller Regel den Wettbewerb auf Ebene des standardisierten Produktes beschränken.
    - Auch die Erarbeitung unverbindlicher Standards kann Wettbewerbsbeschränkungen zulasten von Nichtmitgliedern und privilegienarmen Mitgliedsunternehmen zur Folge haben. Es kommt insoweit auf die Voraussetzungen an, unter denen ein Nichtmitglied oder Mitgliedsunternehmen den Standard inhaltlich (nach Maßgabe seiner eigenen unternehmerischen Interessen) beeinflussen, technisches Wissen (in Bezug auf die optimale Imp-

158 Siehe zusammenfassend etwa Heinemann, CR 2005, 715.

lementierung des Standards) erwerben und den Standard früher als seine Wettbewerber bei der Produktentwicklung berücksichtigen kann. Von Bedeutung sind auch die Voraussetzungen, unter denen ein Anspruch auf die Erteilung von Lizenzen besteht, die zur Nutzung oder Implementierung des Standards erforderlich sind.

  - Werden in einer frühen Phase der Standardisierungstätigkeit grundlegende Standardisierungsentscheidungen durch die Gründungsmitglieder einer Standardisierungsinitiative getroffen, kann von dieser Verhaltenskoordinierung eine irreversible Wettbewerbsbeschränkung zulasten anderer Unternehmen ausgehen.

- Wettbewerbsbeschränkung durch Zugangsbeschränkung

  - Durch die ungerechtfertigte Verweigerung des Zugangs zu Schutzrechten (Nutzungsschutzrechte, Implementierungsschutzrechte etc.) und sonstigen Vorleistungen (Informationssysteme, Datenformate etc.), die für die Teilnahme am Wettbewerb auf IT-Märkten unterlässlich sind, kann ein marktbeherrschendes Unternehmen diesen Wettbewerb beeinträchtigen oder sogar vollständig unterdrücken. Entsprechendes gilt, wenn das marktbeherrschende Unternehmen den Zugang von unangemessenen Bedingungen abhängig macht.

  - Auf Grund der regelmäßig sehr engen Verbindungen zwischen einzelnen IT-Märkten bestehen überdies zahlreiche Ansatzpunkte, um durch Zugangsverweigerungen eine beherrschende Stellung in einem Markt auf andere Märkte zu übertragen.

- Wettbewerbsbeschränkung durch Lizenzierung

  - Werden gewerbliche Schutzrechte erteilt, die zur Nutzung oder Implementierung eines Standards erforderlich sind, kann der Wettbewerb durch die Gestaltung der Lizenzbedingungen beschränkt werden. Zu denken ist u. a. an explizite Wettbewerbsverbote oder an die Erstreckung der Schutzrechtswirkung auf nicht geschützte Leistungsinhalte.

- Wettbewerbsbeschränkung durch Produktkopplung

  - Ein Unternehmen, das auf dem Markt, dem ein bestimmtes Produkt (z. B. ein Betriebssystem) angehört, eine beherrschende Stellung einnimmt, kann den Wettbewerb beschränken, wenn es mit diesem Produkt ein anderes Produkt (z. B. eine Applikation) koppelt und die Kunden keine Möglichkeit haben, die Produkte einzeln zu beziehen.

  - Produktkopplungen können angesichts der Bedeutung patentgeschützter Technologien für IT-Märkte gerade auch in Lizenzverträgen erfolgen.

8.1.2 Beschränkungspotentiale bei „Trusted Computing“

Diese Gefahren für einen unbeschränkten Wettbewerb, mit denen in IT-Märkten angesichts ihrer wirtschaftlichen Besonderheiten allgemein zu rechnen ist, bilden den Rahmen, in dem sich wettbewerbspolitische Risiken auch im Bereich des „Trusted Computing“ ergeben können.

8.1.2.1 Theoretische Literatur

In der theoretischen Literatur wird davon ausgegangen, dass sich viele der allgemeinen Wettbewerbsrisiken auch in den „Trusted Computing“-Märkten manifestieren können.

- Wettbewerbsbeschränkung durch Standardisierung[159]
    - Bei der Ausgestaltung der Kategorien für eine Mitgliedschaft in der TCG werden diskriminierende Effekte zulasten kleiner und mittlerer Unternehmen ausgemacht.[160] Bedenken werden insoweit gegen die starren Mitgliedschaftsgebühren vorgebracht, die im Gegensatz zu entsprechenden Gebühren bei anderen Standardisierungsinitiativen nicht von wirtschaftlichen Kenngrößen abhängig sind.[161] Auch die Einführung einer Kategorie für „Small Adopters“ wird diesbezüglich nicht als ausreichend angesehen.[162] Dies wird damit begründet, dass zum einen mit der Mitarbeiterzahl kein sachgerechtes Kriterium zugrunde gelegt worden sei.[163] Zum anderen ergebe sich die eigentliche Wettbewerbsbeschränkung ohnehin erst aus der Beschränkung des Zugangs zu den höheren Mitgliedschaftskategorien.[164] Darüber hinaus würden die Transaktionskosten, die mit dem Erwerb von gewerblichen Schutzrechten, die zur Implementierung der TCG-Standards benötigt werden, kleine und mittlere Unternehmen tendenziell stärker belasten als ihre größeren Wettbewerber.[165]
    - Neben den Voraussetzungen für die Mitgliedschaft werden darüber hinaus den Weichenstellungen in der Gründungsphase der TCG und ihrer Vorgän-

---

159 Bechtold, CR 2005, 393, 402, weist insoweit darauf hin, dass mit den diesbezüglichen Bedenken allgemeine kartellrechtliche Probleme aufgegriffen würden. Es spricht allerdings viel dafür, dass generell die im Bereich des „Trusted Computing“ erkennbaren Wettbewerbsgefahren, einschließlich der von ihm im Weiteren aufgezeigten Probleme, letzten Endes nur Spielarten bereits bekannter Wettbewerbsbeschränkungen sind.

160 Erber, DIW-Wochenbericht 2007, 517, 520; Koenig/Neumann, DuD 2004, 555, 556; Neumann (Fn. 127), S. 212.

161 Erber, DIW-Wochenbericht 2007, 517, 520; Koenig/Neumann, DuD 2004, 555, 556; Neumann (Fn. 127), S. 212.

162 Neumann, in: Pohlmann/Reimer, Trusted Computing, 2007 (in Drucklegung), S. 220, 232 (voraussichtlich); Neumann (Fn. 127), S. 212; tendenziell a. A. Bechtold, CR 2005, 393, 402.

163 Neumann (Fn. 162), S. 232; Neumann (Fn. 127), S. 212.

164 Neumann (Fn. 162), S. 232 f. Vgl. auch Koenig/Neumann, DuD 2004, S. 555 u. 556.

165 Erber, DIW-Wochenbericht 2007, 517, 520; Neumann (Fn. 127), S. 212.

gerorganisation TCPA wettbewerbsbeschränkende Wirkungen zugemessen.[166] Kritisiert wird, dass insoweit eine kleine Zahl marktstarker Unternehmen die grundlegenden Standardisierungsentscheidungen für die „Trusted Computing"-Technologie getroffen habe, so dass die Bedingungen einer in Zukunft marktzugangsrelevanten Technologie auf einem koordinierten Verhalten einer kleinen Gruppe von Unternehmen beruhen.[167]

- Außerdem wird es für möglich gehalten, dass Microsoft auf Grund seiner beherrschenden Stellung auf dem Markt für Betriebssysteme rein faktisch die Standardisierungsentscheidungen in der TCG nach Maßgabe seiner einzelwirtschaftlichen Interessen beeinflussen kann.[168] Da der Markterfolg von „Trusted Computing" zu einem wesentlichen Teil von einer Unterstützung durch das marktbeherrschende Betriebssystem abhänge, könne Microsoft evtl. auch innerhalb der TCG in der Lage sein, seine Interessen unabhängig von den anderen Mitgliedsunternehmen durchzusetzen und auf diese Weise wettbewerbsfremde Vorteile im Standardisierungsprozess erzielen.[169]

- Wettbewerbsbeschränkung durch Zugangsbeschränkung

  - Zugangsbeschränkungen werden insbesondere hinsichtlich der Schnittstelleninformationen befürchtet, die erforderlich sein werden, um in künftigen Versionen des „Windows"-Betriebssystems dort implementierte „Trusted Computing"-Funktionen nutzen zu können.[170] Entsprechendes gilt für Schnittstellen in Hardwarekomponenten mit „Trusted Computing"-Funktionalität.[171] Auf diese Weise könnte ein marktbeherrschendes Unternehmen den Wettbewerb auf den nachgelagerten Märkten für „Trusted Computing"-Systeme und -Anwendungen behindern.[172]

  - Durch die Bindung von Dateien an bestimmte Systemzustände könnte „Trusted Computing" außerdem dazu genutzt werden, proprietäre Dateiformate zu schaffen und auf diese Weise die Interoperabilität zwischen konkurrierenden Applikationen zu beschränken.[173] Auf diese Weise könnte ein marktbeherrschendes Unternehmen seine Wettbewerber durch die Nutzung der „Trusted Computing"-Technologie behindern.[174]

---

166 Koenig/Neumann, DuD 2004, 555, 556; Neumann (Fn. 162), S. 228; Neumann (Fn. 127), S. 213.
167 Koenig/Neumann, DuD 2004, 555, 556.
168 Koenig/Neumann, DuD 2004, 555, 557; Neumann (Fn. 162), S. 228; Neumann (Fn. 127), S. 214 f.
169 Koenig/Neumann, DuD 2004, 555, 556 f; Neumann (Fn. 127), S. 214.
170 Blaha (Fn. 127), S. 235; Koenig/Neumann, DuD 2004, 555, 556; Neumann (Fn. 162), S. 228.
171 Bechtold, CR 2005, 393, 401.
172 Bechtold, CR 2005, 393, 401; Koenig/Neumann, DuD 2004, 555, 556; Neumann (Fn. 162), S. 228.
173 Bechtold, CR 2005, 393, 401; Müller/Meyer, Wettbewerb und Regulierung in der globalen Internetökonomie – Eine rechtsvergleichende Studie zwischen europäischem und US-amerikanischem Recht, 2007, S. 69.
174 Bechtold, CR 2005, 393, 401; Neumann (Fn. 162), S. 228 (voraussichtlich).

- Des weiteren wird die Gefahr gesehen, dass Microsoft über die Kontrolle der „Trusted Computing“-Schnittstellen und die damit ermöglichten Funktionen der digitalen Rechteverwaltung (Digital Rights Management) seine Marktmacht auf dem Markt für Betriebssysteme nicht nur auf Applikationenebene, sondern darüber hinaus auch auf die Ebene der Inhalte (Musik, Filme etc.) ausdehnen könnte.[175] Entsprechendes gilt für (sonstige) Dienste, die über das Internet angeboten werden.[176]

- Allgemein wird angesichts des potentiell zu beachtenden Patentschutzes auch die Gefahr von Wettbewerbsbeschränkungen durch die Verweigerung des Zugangs zu Schutzrechten unter angemessenen Bedingungen für beachtlich gehalten.[177]

- Wettbewerbsbeschränkung durch Produktkopplung

  - Im Bereich der Produktkopplung wird die Gefahr gesehen, dass, ähnlich wie im Falle des „Media Player“, Microsoft möglicherweise den Wettbewerb auf bestimmten Märkten für „Trusted Computing“-Applikationen oder -Komponenten (Sicherheitssoftware, Virenschutzprogramme etc.) dadurch beschränken kann, dass es diese Applikationen oder Komponenten mit seinem „Windows“-Betriebssystem koppelt.[178]

Bislang nicht spezifisch im Zusammenhang mit „Trusted Computing“ diskutiert wird die Möglichkeit einer Wettbewerbsbeschränkung im Rahmen von Lizenzvereinbarungen. Gerade angesichts der hohen Technologieintensität von Entwicklungen im Bereich des „Trusted Computing“ ist jedoch keineswegs ausgemacht, dass das damit eröffnete Beschränkungspotential ungenutzt bleiben wird.

8.1.2.2 Einschätzungen der Anwendungspraxis

In der Anwendungspraxis wird bislang nur einigen dieser theoretischen Bedenken Bedeutung beigemessen. So wird in der Ergänzung des „Windows“-Betriebssystems um „Trusted Computing“-Komponenten durchaus ein Marktzutrittshindernis für konkurrierende Angebote gesehen.[179] Generell wird erkannt, dass durch die Attestierungsmechanismen von „Trusted Computing“ Hersteller von IT-Plattformen (Rechner, Betriebssysteme, erweiterungsfähige Applikationen etc.) in die Lage versetzt werden, den Wettbewerb auf nachgelagerten Marktstufen zu kontrollieren bzw. auszuschalten.[180]

---

175 Koenig/Neumann, DuD 2004, 555, 557; Müller/Meyer (Fn. 173), S. 70; Neumann (Fn. 162), S. 228 (voraussichtlich).
176 Bechtold, CR 2005, 393, 396; Müller/Meyer (Fn. 173), S. 70.
177 Bechtold, CR 2005, 393, 401.
178 Blaha (Fn. 127), S. 234.
179 Linnemann/Heibel/Pohlmann, in: Pohlmann/Reimer (Fn. 162), S. 72, 76.
180 Hansen/Hansen, in: Pohlmann/Reimer (Fn. 162), S. 208, 212.

Diese Einschätzungen sind aktuellen Veröffentlichungen von Wissenschaftlern entnommen, deren Forschungstätigkeit den Bereich des „Trusted Computing“ umfasst. Demgegenüber fehlt es bemerkenswerterweise an entsprechenden Einlassungen von Unternehmensseite. Vielmehr wurden auch in keinem der zahlreichen Gespräche, die zur Vorbereitung der vorliegenden Studie mit den Marktteilnehmern geführt wurden, wettbewerbspolitische Bedenken geäußert. Obwohl allgemeine und auf Grundlage der in der theoretischen Literatur identifizierten Gefahrenlagen konkretisierte Fragen zu entsprechenden Risiken Bestandteil des verwendeten Fragenkatalogs waren, wurden von keinem der Befragten diesbezügliche Bedenken geäußert.

Lediglich in der Zwischenbesprechung, die studienbegleitend im Bundeswirtschaftsministerium durchgeführt wurde, äußerte einer der teilnehmenden Wissenschaftler die Einschätzung, durch die Bedingungen einer Mitgliedschaft in der TCG in seiner Forschungstätigkeit behindert zu werden, da er hierdurch in der Nutzung von Fachkenntnissen beschränkt werde. Dieser Einschätzung wurde indes von Seiten der anderen Besprechungsteilnehmer widersprochen. Es fanden sich auch keine Hinweise in der Satzung der TCG auf eine über das notwendige Maß hinausgehende Vertraulichkeitsverpflichtung.[181] Es ist daher davon auszugehen, dass die betreffenden Bedenken nicht verallgemeinerungsfähig sind und als Einschätzung eines Vertreters der Forschung insbesondere nicht den hier relevanten Bereich der wettbewerblichen Entfaltung von Wirtschaftsunternehmen betreffen.

8.1.3 Zwischenergebnis

In den dynamischen und komplexen IT-Märkten ist der funktionsfähige Wettbewerb besonderen Gefahren ausgesetzt. Dies wird gerade auch an den zwar zahlenmäßig geringen, aber z. T. grundlegenden Verfahren deutlich, die von der Kommission seit 1980 in diesem Wirtschaftsbereich geführt wurden. Dennoch fehlt es an Hinweisen darauf, dass die Marktteilnehmer innerhalb und außerhalb der TCG bei der Entwicklung der „Trusted Computing“-Technologie tatsächlich entsprechende Wettbewerbsrisiken sehen. Dabei ist unklar, ob solche Wettbewerbsgefahren bewusst verschwiegen werden, ob ihre Wahrnehmung von der Aussicht auf die wettbewerblichen Chancen des „Trusted Computing“ überlagert wird, oder ob es sie tatsächlich nicht gibt.

Letzteres stünde in einem kaum erklärbaren Widerspruch zu den Erkenntnissen aus anderen IT-Märkten. Die theoretische Literatur hat demzufolge auch mehrere potentielle Wettbewerbsbeschränkungen identifiziert. So werden auf Ebene der Standardisierung diskriminierende Effekte zulasten kleiner und mittlerer Unternehmen durch die Ausgestaltung der Mitgliedschaft in der TCG, uneinholbare Wettbewerbsvorsprünge der Grün-

181 Siehe dazu Abschnitt 15.3 der TCG-Satzung, der zahlreiche Ausnahmen von der Vertraulichkeitsverpflichtung vorsieht.

dungsmitglieder und die Gefahr der Steuerung des Standardisierungsprozesses durch Microsoft geltend gemacht.

Daneben werden wettbewerbspolitische Gefahren bei der Gestaltung eines „Trusted Computing“-Betriebssystems durch ein marktbeherrschendes und vertikal integriertes Softwareunternehmen gesehen: Hier drohen Zugangsbeschränkungen hinsichtlich notwendiger Schnittstelleninformationen, durch die die bestehende Marktmacht mit Hilfe der DRM-Funktionalitäten von „Trusted Computing“ sogar auf nachgelagerte Inhalte- und Dienstemärkte ausgedehnt werden könnte.

Außerdem könnte der Wettbewerb auf nachgelagerten „Trusted Computing“-Applikationsmärkten (für Sicherheitssoftware, Virenschutzprogramme etc.) durch die Kopplung entsprechender Komponenten an ein marktdominantes Betriebssystem beschränkt werden. Nicht ausgeschlossen sind auch Wettbewerbsbeschränkungen durch die Verweigerung von Lizenzen für notwendige „Trusted Computing“-Technologiekomponenten zu angemessenen Bedingungen sowie im Rahmen entsprechender Lizenzvereinbarungen.

8.2 Reaktionsmöglichkeiten

Die wettbewerbspolitischen Risiken, die von den Entwicklungen im Bereich des „Trusted Computing“ ausgehen, müssen keineswegs in entsprechenden Wettbewerbsbeschränkungen resultieren. Inwieweit es dazu kommt, hängt in allererster Linie davon ab, ob diejenigen Marktteilnehmer, die über entsprechende Möglichkeiten zur Beschränkung des Wettbewerbs verfügen, von diesen auch tatsächlich Gebrauch machen werden.

Den hiervon potentiell betroffenen Marktteilnehmern selbst stehen diesbezüglich allerdings kaum wirksame Reaktionsmöglichkeiten zur Verfügung. Zwar könnte etwa die Einrichtung eines Technologiepools die potentiellen Nachteile kleiner und mittlerer Unternehmen, denen diese beim Zugriff auf die TCG-Technologie ausgesetzt sind, partiell kompensieren.[182] Die Einrichtung eines solchen Pools hängt aber von einer entsprechenden Initiative derjenigen Unternehmen ab, die sich durch die Errichtung eines wettbewerbskonformen Technologiepools selbst der ihnen eröffneten Möglichkeiten zur Beschränkung des Wettbewerbs begeben müssten.[183]

Einer gerichtlichen Durchsetzung des Wettbewerbsrechts durch die von etwaigen Verletzungen betroffenen Marktteilnehmer selbst stehen schließlich weitgehende Darle-

---

182 Koenig/Neumann, DuD 2004, 555, 558 f.; Neumann (Fn. 127), S. 212 f.

183 Demzufolge fehlt es, soweit ersichtlich, an einer entsprechenden Bereitschaft, vgl. Bechtold, CR 2005, 393, 401; Neumann (Fn. 127), S. 213.

gungs- und Beweislasten entgegen.[184] Dem damit einhergehenden Prozess- und Kostenrisiko stehen nur sehr eingeschränkte Möglichkeiten dieser Unternehmen gegenüber, die zur Darlegung und zum Nachweis entsprechender Rechtsverletzungen benötigten Auskünfte und Informationen zu erlangen.[185] Demzufolge bestätigt auch die wettbewerbsrechtliche Praxis, dass generell,[186] insbesondere aber auch in IT-Märkten die von Wettbewerbsverstößen potentiell betroffenen Marktteilnehmer die Wettbewerbsregeln nicht selbst durchsetzen.[187]

Damit stellt sich vorrangig die Frage nach den diesbezüglichen Reaktionsmöglichkeiten staatlicher Instanzen. Dabei soll der Schutz des unbeschränkten Wettbewerbs nachfolgend als Anlass und Ausgangspunkt der Darstellung dienen. An geeigneter Stelle soll aber zugleich kurz darauf eingegangen werden, inwieweit staatliche Maßnahmen auch zur Durchsetzung anderer öffentlicher Interessen im Bereich des „Trusted Computing" dienen können. Zu denken wäre hier beispielsweise an die Wahrung der informationellen Selbstbestimmung, also an die Durchsetzung datenschutzfreundlicher Technikgestaltung, und an sicherheitspolitische Interessen in dem essentiellen Bereich der IT-Infrastruktur.

8.2.1 Wettbewerbsrecht

Das bedeutsamste Instrument zum Schutz des Wettbewerbs ist naturgemäß das Wettbewerbsrecht.

8.2.1.1 Allgemeine Steuerungswirkung der wettbewerbsrechtlichen Normen

Insoweit sind die wettbewerbsrechtlichen Verbotsnormen selbst bereits ein wichtiges Steuerungsinstrument von potentiell erheblicher Effektivität. Sowohl dem Kartellverbot als auch dem Missbrauchsverbot kommt ein unmittelbarer Geltungs- und Befolgungsanspruch zu.[188] An die Verletzung dieser normativen Verbote sind potentiell weitreichende Rechtsfolgen geknüpft: Neben der Möglichkeit behördlicher Maßnahmen treten – jedenfalls nach deutschem Wettbewerbsrecht – Beseitigungs-, Unterlassungs- und Schadensersatzansprüche betroffener Marktteilnehmer[189] sowie eine Sanktionierung vorsätzlicher und fahrlässiger Verstöße als Bußgeldtatbestände.[190]

---

184 Vgl. etwa Bechtold, in: Bechtold, Kartellgesetz, 4. A., 2006, § 19 Rn. 94, und für das EG-Wettbewerbsrecht die ausdrückliche Regelung in Art. 2 der Wettbewerbsverordnung 1/2003.
185 Vgl. etwa Bechtold/Bosch/Brinker/Hirsbrunner, EG-Kartellrecht, 2005, Art. 2 VO 1/2003 Rn. 10 u. 12.
186 Möschel, ZWeR 2007, 261, 264: „In Europe, private enforcement is hitherto practically non-existent."
187 So wurden bezeichnenderweise die wettbewerbsrechtlichen Aspekte in den oben, unter 8.1.1.1.1 , nachgewiesenen Verfahren vor den deutschen Zivilgerichten nicht von der jeweils klagenden Partei in den Prozess eingeführt, sondern (zur Verteidigung) von den dortigen Beklagten.
188 Koenig/Loetz/Neumann (Fn. 121), S. 51.
189 § 33 GWB.
190 § 81 Abs. 1 i. V. m. Art. 81 u. 82 EG sowie § 81 Abs. 2 Nr. 1 i. V. m. §§ 1, 19, § 20 Abs. 1 GWB.

Darüber hinaus sind Rechtsgeschäfte, die unter Verstoß gegen eine Verbotsvorschrift des Wettbewerbsrechts getätigt wurden, nach deutschem Recht i. d. R. nichtig.[191] Hinzu kommen schließlich die potentiell negativen Konsequenzen für die Reputation eines Unternehmens, wenn ein Verstoß gegen das Wettbewerbsrecht bekannt wird. Für die Unternehmen bestehen also erhebliche rechtliche und wirtschaftliche Anreize, sich an die wettbewerbsrechtlichen Vorgaben zu halten.

Allerdings kennzeichnet die gesetzlichen Vorgaben ein sehr hoher Abstraktionsgrad.[192] Dies erschwert (auch) den normunterworfenen Marktteilnehmern die Beurteilung, ob ein bestimmtes Verhalten in Konflikt mit den wettbewerbsrechtlichen Vorgaben gerät. Erkennt ein Marktteilnehmer aber bereits nicht, dass sein Verhalten wettbewerbsrechtlich bedenklich sein kann, läuft die von den normativen Vorgaben ausgehende Steuerungswirkung faktisch leer. Dieses Problem hat auch die wettbewerbsrechtliche Praxis erkannt. Sie versucht, ihm mit der Veröffentlichung von Leitlinien und Auslegungshinweisen zu begegnen, in denen die jeweils zuständigen Wettbewerbsbehörden auf europäischer und mitgliedstaatlicher Ebene erläutern, wie sie die Vorschriften des Wettbewerbsrechts allgemein oder in bestimmten Wirtschaftszweigen handhaben.[193]

Solche Leitlinien und Auslegungshinweise beruhen i. d. R. auf keiner formellen Ermächtigungsgrundlage. Ihnen kommt daher keine unmittelbare rechtliche Wirkung zu. Eine solche kann sich erst – mittelbar – aus der tatsächlichen Anwendung dieser Grundsätze ergeben, die mit Blick auf den Gleichbehandlungsgrundsatz eine gewisse Selbstbindung des behördlichen Ermessens zur Folge hat. In jedem Fall dürfte ein Unternehmen durch die Befolgung solcher behördlichen Leitlinien und Auslegungshinweise die verkehrsübliche Sorgfalt wahren und damit zumindest die tatsächlich besonders empfindlichen Folgen vermeiden können, die an einen Verstoß gegen die wettbewerbsrechtlichen Vorgaben geknüpft sind (Schadensersatzansprüche, Bußgelder).

Da die wettbewerbsrechtlichen Risiken, die bei „Trusted Computing“ bestehen, einen erheblichen Komplexitätsgrad aufweisen, könnte die Veröffentlichung spezifischer Anwendungsgrundsätze einen bedeutsamen Beitrag zur Effektivierung der wettbewerbsrechtlichen Vorgaben in diesem Bereich bedeuten. Solche Leitlinien oder Auslegungshinweise müssten allerdings von der jeweils zuständigen Wettbewerbsbehörde veröffentlicht werden. Nur auf diese Weise würden sie zum einen als praktisch maßgebliche Vorgaben anerkannt werden und könnten zum anderen auch die hierfür ebenfalls förderliche Rechtswirkung (in Form einer Selbstbindung des behördlichen Ermessens) erzeugen.

---

191 Bechtold (Fn. 184), Vorbem. zu § 32 Rn. 1.
192 Koenig/Loetz/Neumann (Fn. 121), S. 51.
193 Vgl. Bechtold/Bosch/Brinker/Hirsbrunner (Fn. 185), Art. 2 VO 1/2003 Rn. 25.

8.2.1.2 Wettbewerbsbehördliche Maßnahmen

Trotz der erheblichen Anreize für ein normgerechtes Verhalten lehrt die wettbewerbsrechtliche Praxis, dass gegen das Kartell- und gegen das Missbrauchsverbot verstoßen wird. In einem solchen Fall kommt der Möglichkeit eines Eingreifens der zuständigen Wettbewerbsbehörde schon angesichts der dargestellten Begrenzungen privater Rechtsdurchsetzungsinstrumente erhebliche Bedeutung zu.

8.2.1.2.1 Eingriffsvoraussetzungen und Eingriffsziele

Voraussetzung für einen wettbewerbsbehördlichen Eingriff ist, dass eine Verletzung der wettbewerbsrechtlichen Vorschriften vorliegt.[194] Damit ist zum einen verbunden, dass grundsätzlich gegen jede Verletzung des Wettbewerbsrechts auf wettbewerbsrechtlicher Grundlage vorgegangen werden kann. Zugleich können wettbewerbsrechtliche Maßnahmen deshalb aber ausschließlich der Durchsetzung des Wettbewerbsrechts dienen. Ungeachtet der nicht unstrittigen Frage, was unter Wettbewerb im Einzelnen zu verstehen ist, besteht insoweit Einigkeit, dass das Wettbewerbsrecht nur dem Schutz des Wettbewerbs auf dem Markt dient.[195]

Aber auch bei der Ausübung des bestehenden Aufgreifermessens („kann“) der jeweils zuständigen Wettbewerbsbehörde[196] wird es i. d. R. ausgeschlossen sein, maßgeblich Gesichtspunkte heranzuziehen, die nicht den Zwecken des Gesetzes entsprechen,[197] hier also den Zwecken des Wettbewerbsrechts und damit dem Schutz des Wettbewerbs.[198] Durch wettbewerbsbehördliche Maßnahmen können außerwettbewerbliche Zielsetzungen, wie etwa die Durchsetzung datenschutzrechtlicher oder sicherheitspolitischer Interessen, mithin nicht unmittelbar verfolgt werden. Demgegenüber ist ein Tätigwerden der Wettbewerbsbehörden nicht schon dann ausgeschlossen, wenn die Wettbewerbsbeschränkung (ggf. ausschließlich) von einem oder mehreren Unternehmen ausgeht, die außerhalb des Hoheitsbereichs der EG ansässig sind. Denn nach überwiegender Auffassung gilt für das europäische Wettbewerbsrecht das sog. Auswirkungsprinzip, das auch der Anwendungspraxis der Kommission zugrunde liegt und für das es alleine darauf ankommt, ob sich die potentiell wettbewerbsbeschränkende Wirkung innerhalb der EG auswirkt.[199]

---

194 Siehe § 32 Abs. 1 GWB u. Art. 7 Abs. 1 S. 1 der Wettbewerbsverordnung 1/2003.
195 Siehe Erwägungsgrund 9 S. 1 der Wettbewerbsverordnung 1/2003.
196 Für § 32 Abs. 1 GWB: Bechtold (Fn. 184), § 32 Rn. 4; für Art. 7 Abs. 1 der Wettbewerbsverordnung 1/2003: Bechtold/Bosch/Brinker/Hirsbrunner (Fn. 185), Art. 7 VO 1/2003 Rn. 27 (hinsichtlich des Einleitens einer Untersuchung) u. Rn. 28 (hinsichtlich des Erlasses einer Abstellungsentscheidung).
197 Kopp/Ramsauer, VwVfG, 9. A., 2005, § 40 Rn. 24a.
198 Siehe hierzu auch Möschel, ZWeR 2007, 261, 263. Vgl. hinsichtlich der konkreten Ausübung von Ermittlungsbefugnissen auch Bechtold (Fn. 184), § 59 Rn. 5 (keine Inanspruchnahme der wettbewerbsrechtlichen Auskunftsbefugnisse „für einen außerkartellrechtlichen Zweck“).
199 Vgl. Weiß, in: Calliess/Ruffert, EUV/EGV, 3. A., 2007, Art. 81 EGV Rn. 8 ff. m. w. N.

8.2.1.2.2 Verfahrensdurchführung

Auch die Wirksamkeit und Ausgestaltung wettbewerbsbehördlicher Verfahren wird zunächst maßgeblich von der Verteilung der Beweislast für die einzelnen Voraussetzungen eines Verstoßes gegen das Wettbewerbsrecht bestimmt. Diese trifft ganz überwiegend die Wettbewerbsbehörden.[200] Die Unternehmen, die potentiell gegen das Wettbewerbsrecht verstoßen, sind nur hinsichtlich ganz bestimmter Aspekte beweisbelastet, die sie ausnahmsweise von dem Verdikt eines Verstoßes gegen das Wettbewerbsrecht bewahren.[201] Daneben besteht auch eine weitreichende formelle Beweislast der Wettbewerbsbehörden. Diese verlangt eine weitestmögliche Ausforschung des Sachverhaltes auch dort, wo die materielle Beweislast bei den Unternehmen liegt, denen der Verstoß gegen das Wettbewerbsrecht zur Last gelegt wird.

Im Gegensatz zu den anderen Marktteilnehmern stattet das Wettbewerbsrecht die Wettbewerbsbehörden indes mit hoheitlichen Ermittlungsbefugnissen aus, die es ihnen erheblich erleichtern, ihrer formellen (und weitgehend auch materiellen) Beweislast zu genügen. Das umfasst insbesondere weitreichende Auskunfts- und Nachprüfungsbefugnisse.[202] Diese Ermittlungsbefugnisse dürfen aber immer nur im Zusammenhang mit einem konkreten Untersuchungsgegenstand ausgeübt werden.[203]

Es bedarf somit grundsätzlich eines (belastbaren) Anfangsverdachtes, dass gegen das Kartell- oder Missbrauchsverbot tatsächlich verstoßen wird, um auf Grundlage dieser Befugnisse Ermittlungen im Bereich des „Trusted Computing“ aufzunehmen.[204] Daneben sehen sowohl das deutsche als auch das europäische Wettbewerbsrecht die Möglichkeit einer so genannten Enqueteuntersuchung vor. Eine solche ist immer schon dann möglich, wenn bestimmte Umstände *vermuten* lassen, dass der Wettbewerb möglicherweise beschränkt ist.[205] Bei einer solchen Enqueteuntersuchung kann die Wettbewerbsbehörde unter Inanspruchnahme entsprechender Auskunfts- und Nachprü-

---

200 Siehe mit Blick auf das GWB etwa Bechtold (Fn. 184), § 19 Rn. 53 u. 58 (für die – auch im Rahmen von § 20 Abs. 1 GWB anwendbaren, Bechtold (Fn. 184), § 20 Rn. 10 – Vermutungsregeln des § 19 Abs. 3 GWB), und aus gemeinschaftsrechtlicher Sicht Art. 2 der Wettbewerbsverordnung 1/2003; Bechtold/Bosch/Brinker/Hirsbrunner (Fn. 185), Art. 2 VO 1/2003 Rn. 10.

201 Das betrifft jedenfalls nach deutschem Wettbewerbsrecht etwa die Beweislast für die sachliche Rechtfertigung eines grundsätzlich wettbewerbswidrigen Verhaltens, vgl. etwa zu § 19 Abs. 4 Nr. 3 GWB BGH, Beschl. v. 22.7.1999 – Az. KVR 12/98, BGHZ 142, 239, 246 – Flugpreisspaltung; Bechtold (Fn. 184), § 19 Rn. 84. Auf Unternehmensseite liegt auch die Beweislast für das Vorliegen der Freistellungsvoraussetzungen vom Kartellverbot nach Art. 81 Abs. 3 EG, wohingegen die Beweislast für das Nichtvorliegen dieser Voraussetzung nach § 2 Abs. 1 GWB die Wettbewerbsbehörde trifft, siehe Bechtold (Fn. 184), § 2 Rn. 6.

202 §§ 57 – 59 GWB u. Art. 18 – 20 der Wettbewerbsverordnung 1/2003.

203 Für § 59 GWB Emmerich, Kartellrecht, 10. A., 2006, § 41 Rn. 6 (S. 503); implizit auch Bechtold (Fn. 184), § 59 Rn. 4; für Art. 18 der Wettbewerbsverordnung 1/2003 Bechtold/Bosch/Brinker/Hirsbrunner (Fn. 185), Art. 18 VO 1/2003 Rn. 2. Siehe auch Art. 20 Abs. 8 S. 2 der Wettbewerbsverordnung 1/2003.

204 Für § 59 GWB OLG Düsseldorf, Beschl. v. 11.6.2003 – Az. Kart 7/03 (V), WuW/E DE-R 1179, 1180 – Stromcontracting; Bechtold (Fn. 184), § 59 Rn. 6.

205 § 32e Abs. 1 GWB u. Art. 17 Abs. 1 UAbs. 1 S. 1 der Wettbewerbsverordnung 1/2003.

fungsbefugnisse[206] einen gesamten Wirtschaftszweig oder (sektorübergreifend) eine bestimmte Art von Vereinbarungen untersuchen.

Die nur theoretische Gefahr einer solchen Wettbewerbsbeschränkung reicht demgegenüber nicht aus. Damit wettbewerbsbehördliche Ermittlungen im Bereich des „Trusted Computing“ möglich sind, müssen also tatsächliche Umstände darauf hindeuten, dass durch Vereinbarungen oder abgestimmte Verhaltensweisen der Wettbewerb beschränkt wird bzw. dass ein marktbeherrschendes Unternehmen seine Marktmacht missbraucht. Insoweit bestehen allerdings keine allzu strengen Anforderungen.[207] Dies gilt namentlich für die Möglichkeit einer Enqueteuntersuchung, die bereits gegeben ist, wenn sich aus den konkreten Umständen die *Vermutung* einer eventuellen Wettbewerbsbeschränkung ergibt. Auf Grundlage der Erkenntnisse einer Enqueteuntersuchung können dann einzelne Kartell- oder Missbrauchsverfahren eingeleitet werden.

8.2.1.2.3 Wettbewerbsschützende Maßnahmen

Kommt es zur Durchführung eines wettbewerbsbehördlichen Verfahrens und ggf. entsprechender Ermittlungen, sind auf Grundlage eines solchen Verfahrens verschiedene Maßnahmen gegen etwaige Wettbewerbsbeschränkungen möglich.

8.2.1.2.3.1 Einstweilige Maßnahmen

Noch vor Abschluss eines Kartell- oder Missbrauchsverfahrens können die Wettbewerbsbehörden in dringenden Fällen, wenn die Gefahr eines ernsten, nicht wiedergutzumachenden Schadens für den Wettbewerb besteht, einstweilige Maßnahme erlassen.[208] Voraussetzung ist hierfür zunächst, dass das Verhalten des betreffenden Unternehmens nach erster Prüfung gegen die wettbewerbsrechtlichen Vorgaben verstößt.[209] Die Anforderungen an die Feststellung des potentiellen Verstoßes gegen das Wettbewerbsrecht sind gegenüber einer endgültigen Maßnahme deutlich abgeschwächt.[210] Es reicht aus, dass das beanstandete Verhalten auf den ersten Blick ernsthafte Zweifel an seiner Vereinbarkeit mit dem Wettbewerbsrecht weckt.[211]

Des Weiteren muss ein dringender[212] Fall vorliegen und ohne die Maßnahme ein ernster,[213] nicht wiedergutzumachender[214] Schaden für den Wettbewerb bestehen. Die

---

206 § 32e Abs. 2 S. 1 GWB u. Art. 17 Abs. 1 UAbs. 1 S. 2 der Wettbewerbsverordnung 1/2003.
207 OLG Düsseldorf, Beschl. v. 11.6.2003 – Az. Kart 7/03 (V), WuW/E DE-R 1179, 1180 – Stromcontracting.
208 § 32a Abs. 1 GWB, Art. 8 Abs. 1 der Wettbewerbsverordnung 1/2003.
209 Bechtold (Fn. 184), § 32a Rn. 3.
210 Bechtold (Fn. 184), § 32a Rn. 5.
211 Bechtold ebd.
212 Es muss also sofortiges Handeln notwendig sein.
213 Ernst ist der Schaden, wenn er von erheblicher volkswirtschaftlicher Bedeutung bzw. unerträglich wäre.
214 Nicht wiedergutzumachen ist ein Schaden insbesondere dann, wenn er durch die abschließende Entscheidung nicht mehr beseitigt werden könnte, EuGH, Beschl. v. 17.1.1980 – Rs. 792/79 R,

einstweilige Maßnahme darf nur vorläufiger und sichernder Art sein und muss auf das nach der gegebenen Sachlage Notwendige beschränkt bleiben.[215] Darüber hinaus sind einstweilige Maßnahmen zu befristen.[216] Diese Befristung kann allerdings verlängert werden.[217]

Gerade die letztgenannten zeitlichen Begrenzungen zeigen, dass einstweilige Maßnahmen grundsätzlich erst dann ergriffen werden dürfen, wenn in absehbarer Zeit mit einer Hauptsacheentscheidung gerechnet werden kann. Die Zweifel an der Rechtmäßigkeit des potentiell wettbewerbsbeschränkenden Verhaltens müssen also schon weitgehend verdichtet und hinreichend durch Tatsachenmaterial substantiiert sein. Gerade wenn in Ermittlungsverfahren bei potentiellen Wettbewerbsbeschränkungen im Bereich des „Trusted Computing“ die Aufklärung komplexer tatsächlicher Hintergründe erforderlich ist, werden einstweilige Maßnahmen daher jedenfalls in einem frühen Verfahrensstadium i. d. R. nicht zulässig sein. Je länger die Ermittlungen dauern, desto wahrscheinlicher ist indes, dass der irreversible Schaden für den Wettbewerb bereits eingetreten ist und der bis zum Ergehen der endgültigen Entscheidung noch zu verhindernde Schaden für sich genommen die einstweilige Maßnahme nicht (mehr) rechtfertigen kann.

8.2.1.2.3.2 Abhilfemaßnahmen

Stellt eine Wettbewerbsbehörde abschließend fest, dass tatsächlich eine Verletzung des Wettbewerbsrechts vorliegt, kann sie gegenüber den betreffenden Unternehmen bzw. Unternehmensvereinigungen die Verpflichtung aussprechen, die festgestellte Zuwiderhandlung abzustellen.[218] Sie kann ihnen hierzu alle Maßnahmen aufgeben, die für eine wirksame Abstellung der Zuwiderhandlung erforderlich und gegenüber dem festgestellten Verstoß verhältnismäßig sind.[219] Der Kreis der Abhilfemaßnahmen, die bei etwaigen Wettbewerbsbeschränkungen im Bereich von „Trusted Computing“ in Betracht

---

Slg. 1980, 119, 130 (Rn. 14) – Camera Care/Kommission; Bechtold (Fn. 184), § 32a Rn. 7; Bechtold/Bosch/Brinker/Hirsbrunner (Fn. 185), Art. 8 VO 1/2003 Rn. 6.

215 Bechtold (Fn. 184), § 32a Rn. 9; Bechtold/Bosch/Brinker/Hirsbrunner (Fn. 185), Art. 8 VO 1/2003 Rn. 12. Vgl. auch EuGH, Urt. v. 28.2.1984 – verb. Rs. 228 u. 229/82, Slg. 1984, 1129, 1161 (Rn. 19) – Ford/Kommission.

216 § 32a Abs. 2 S. 1 GWB, Art. 8 Abs. 2 der Wettbewerbsverordnung 1/2003.

217 § 32a Abs. 2 S. 2 GWB, Art. 8 Abs. 2 der Wettbewerbsverordnung 1/2003. Dabei sollen einstweilige Maßnahmen deutscher Wettbewerbsbehörden grundsätzlich insgesamt nicht länger als für die Dauer eines Jahres getroffen werden (§ 32a Abs. 2 S. 3 GWB).

218 § 32 Abs. 1 GWB, Art. 7 Abs. 1 S. 1 der Wettbewerbsverordnung 1/2003.

219 § 32 Abs. 2 GWB, Art. 7 Abs. 1 S. 2 der Wettbewerbsverordnung 1/2003. Neben die Abhilfemaßnahmen tritt schließlich die Möglichkeit, ein Bußgeld zu verhängen. Das diesbezügliche Verfahren weist jedoch gegenüber dem Verfahren zur Abstellung von Wettbewerbsverstößen einige Besonderheiten auf. Da der Verhängung eines Bußgeldes überdies primär Sanktionscharakter zukommt, soll daher im Rahmen der vorliegenden Untersuchung, die auf eine Analyse der Möglichkeiten gerichtet ist, etwaige Wettbewerbsbeschränkungen im Bereich des „Trusted Computing“ zu verhindern, auf eine Darstellung der diesbezüglichen Befugnisse der Wettbewerbsbehörden verzichtet werden. Zu erwähnen ist des Weiteren die nach deutschem Recht bestehende Möglichkeit einer Vorteilsabschöpfung (§ 34 GWB), der angesichts des Erfordernisses schuldhaften Verhaltens aber ebenfalls eher Sanktionscharakter – wenn auch verwaltungsrechtlicher Natur – zukommt, vgl. Bechtold (Fn. 184), § 34 Rn. 2.

kommen, ist somit grundsätzlich sehr weit gezogen. Ausgehend von der wettbewerbsrechtlichen Praxis im IT-Bereich kommen insbesondere folgende Verpflichtungen in Betracht:

- Gewährung des Zugangs zu bestimmten Informationen oder Einrichtungen,[220] insbesondere: Offenlegung von Schnittstelleninformationen (und regelmäßige Aktualisierung dieser Informationen in angemessener Zeit),
- Erteilung von Lizenzen zu vernünftigen und nicht diskriminierenden Bedingungen,[221] insbesondere: Erlaubnis der Implementierung bestimmter Standards zu vernünftigen und nicht diskriminierenden Bedingungen,
- Angebot von Endkundenprodukten (z. B. Betriebssystem) zumindest auch ohne ein hieran gekoppeltes weiteres Endkundenprodukt,
- Änderung von Preis- oder Rabattsystemen oder von Geschäftsbedingungen.[222]

Eine faktische Begrenzung der wettbewerbsbehördlichen Möglichkeiten ergibt sich jedoch daraus, dass alle Maßnahmen auf eine Abstellung der festgestellten Zuwiderhandlung gerichtet sein müssen. Der mögliche Inhalt etwaiger Abhilfemaßnahmen wird somit von der festgestellten Wettbewerbsbeschränkung bestimmt. Angesichts der Vielgestaltigkeit der potentiellen Beschränkungsmöglichkeiten im Bereich des „Trusted Computing“ werden den betroffenen Unternehmen damit erhebliche Ausweichstrategien eröffnet. Zwar können Abhilfemaßnahmen auch das Verbot eines künftigen gleichartigen Verhaltens umfassen.[223] Die Grenze zwischen gleichartigen und ungleichartigen Verhaltensweisen wird jedoch im Einzelfall nicht leicht zu ziehen sein. Oftmals wird sich die (zeitaufwendige) Durchführung eines zweiten Verfahrens nicht vermeiden lassen.[224]

Zu beachten ist weiterhin, dass Abhilfemaßnahmen einer Wettbewerbsbehörde der gerichtlichen Überprüfung unterliegen. Aufschiebende Wirkung kommt einem entsprechenden Rechtsmittel allerdings bei den hier in Rede stehenden Maßnahmen mittlerweile von Gesetzes wegen generell nicht mehr zu.[225] Das gilt seit der Streichung von § 64 Abs. 1 Nr. 1 GWB zum 22. Dezember 2007[226] auch dann, wenn es um eine Abhilfemaßnahme des Bundeskartellamtes mit Bezug auf den Missbrauch einer marktbeherrschenden Stellung geht.

---

220 Vgl. Emmerich (Fn. 203), § 13 Rn. 10 (S. 181).
221 Vgl. Emmerich ebd.
222 Vgl. Emmerich ebd.
223 EuG, Urt. v. 6.10.1994 – Rs. T-83/91, Slg. 1994, II-755, 850 f. (Rn. 220 f.) – Tetra Pak/Kommission; Bechtold/Bosch/Brinker/Hirsbrunner (Fn. 185), Art. 7 VO 1/2003 Rn. 14.
224 Vgl. für das Kartellverbot Bechtold/Bosch/Brinker/Hirsbrunner (Fn. 185), Art. 7 VO 1/2003 Rn. 14, und für das Missbrauchsverbot: BGH, Beschl. v. 24.9.2002 – Az. KVR 15/01, BGHZ 152, 82, 94 ff. – Puttgarden III; Emmerich (Fn. 203), § 43 Rn. 13 (S. 510).
225 Siehe für Abhilfemaßnahmen der Kommission Art. 242 S. 1 EG. Vgl. auch Bechtold (Fn. 184), § 64 Rn. 11.
226 Art. 1 Nr. 13 des Gesetzes zur Bekämpfung von Preismissbrauch im Bereich der Energieversorgung und des Lebensmittelhandels, BGBl. I 2007, 2966.

Dennoch spricht alles dafür, dass behördliche Abhilfemaßnahmen im Falle von „Trusted Computing“ zumindest i. d. R. erst nach Durchführung eines zeitaufwendigen Ermittlungsverfahrens ergehen können. Das ergibt sich schon aus der Komplexität der technischen, wirtschaftlichen und auch rechtlichen Fragestellungen. Hinzu kommt, dass die umfassende Beurteilung eines wettbewerbsrechtlichen Sachverhaltes in IT-Märkten angesichts der dort typischerweise vorliegenden Wettbewerbsbeschränkungen oftmals einen detaillierten Einblick in unternehmensinterne Unterlagen und Informationen erfordert. Hieraus ergibt sich zusätzliches Verzögerungs- und Verdunkelungspotential für die betroffenen Unternehmen. Es ist deshalb zweifelhaft, ob wettbewerbsbehördliche Abhilfemaßnahmen zur Behebung von Wettbewerbsbeschränkungen in den IT-Märkten tatsächlich wirksam beitragen können.[227]

Dem entspricht die wohl bedeutsamste praktische Erfahrung, dass es nur in einer sehr geringen Anzahl von Fällen zu kartellbehördlichen Maßnahmen in IT-Märkten – und dann nach jahrelanger Ermittlungstätigkeit – gekommen ist.[228] An höchstinstanzlichen Leitentscheidungen der deutschen und europäischen Gerichte fehlt es schließlich gänzlich. So wurde namentlich die Leitentscheidung zur Reichweite wettbewerbsrechtlicher Zugangsansprüche gegenüber immaterialgüterrechtlich geschützten Positionen zu einem Sachverhalt aus dem Bereich der pharmazeutischen Industrie,[229] nicht aber zu einem Sachverhalt mit IT-Bezug getroffen und mittlerweile lediglich in der erstinstanzlichen Rechtsprechung auch auf die IT-Branche bezogen.[230]

8.2.1.2.3.3 Verpflichtungszusagen

Als Alternative zu einer rechtsförmlichen Abhilfeentscheidung hat in der Praxis schließlich die Einstellung wettbewerbsbehördlicher Verfahren durch Verpflichtungszusagen der betroffenen Unternehmen große Bedeutung erlangt. Mittlerweile kann die Kartellbehörde eine solche Verpflichtungszusage sogar für bindend erklären,[231] wenn sie sich im Gegenzug verpflichtet, keine Abhilfemaßnahme zu erlassen.[232]

Voraussetzung für eine Verpflichtungszusage ist i. d. R., dass die Wettbewerbsbehörde den betroffenen Unternehmen ihre vorläufige Beurteilung des – weitestmöglich aufgeklärten[233] – Sachverhaltes[234] mitteilt.[235] Erfährt ein Unternehmen auf Grund einer solchen Mitteilung oder durch eine Abmahnung nach vollständigem Abschluss der wettbewerbsbehördlichen Ermittlungen von der (vorläufigen) Einschätzung der Wettbewerbsbehörde, hat es die Möglichkeit, der Behörde Verpflichtungzusagen anzubie-

---

227 Siehe auch Bechtold, CR 2005, 393, 397.
228 Siehe dazu ausführlich oben, unter (S.8.2.1.2.3.3 ff.).
229 EuGH, Urt. v. 29.4.2004 – Rs. C-418/01, Slg. 2004, I-5039 – IMS Health.
230 EuG, Urt. v. 17.9.2007 – Rs. T-201/04.
231 § 32b Abs. 1 S. 1 GWB, Art. 9 Abs. 1 S. 1 der Wettbewerbsverordnung 1/2003.
232 § 32b Abs. 1 S. 2 GWB, Art. 9 Abs. 1 S. 2 der Wettbewerbsverordnung 1/2003.
233 Bechtold (Fn. 184), § 32b Rn. 3; Bechtold/Bosch/Brinker/Hirsbrunner (Fn. 185), Art. 9 VO 1/2003 Rn. 5 f.
234 Bechtold (Fn. 184), § 32b Rn. 3; Bechtold/Bosch/Brinker/Hirsbrunner (Fn. 185), Art. 9 VO 1/2003 Rn. 4 u. 6.
235 Bechtold (Fn. 184), § 32b Rn. 3; Bechtold/Bosch/Brinker/Hirsbrunner (Fn. 185), Art. 9 VO 1/2003 Rn. 7.

ten.[236] Diese Zusagen müssen geeignet sein, die Bedenken der Wettbewerbsbehörde vollständig auszuräumen.[237]

Verpflichtungszusagen sind aus Sicht der Wettbewerbsbehörde reizvoll, weil sie die Risiken einer gerichtlichen Aufhebung einer Abhilfemaßnahme beseitigen, die gerade im IT-Bereich angesichts der komplexen tatsächlichen Zusammenhänge und der selten eindeutigen rechtlichen Bewertung oftmals sehr hoch sind. Darüber hinaus können Gefahren für den Wettbewerb durch Verpflichtungszusagen abgestellt werden, noch bevor die oftmals zeitaufwendigen Verfahren vollständig abgeschlossen sind. Allerdings ist jenseits informeller Verpflichtungszusagen der zu erwartende Zeitgewinn auch nicht zu überschätzen, da der entscheidungsrelevante Sachverhalt grundsätzlich vollständig ermittelt werden muss. Durch die Möglichkeit, unter bestimmten Umständen ein Verfahren auch nach Annahme der angebotenen Verhaltenszusagen wieder aufzunehmen,[238] behält die Wettbewerbsbehörde schlussendlich auch die notwendige Flexibilität, um ggf. doch im Wege einer förmlichen Abhilfemaßnahme vorgehen zu können.

Von dieser Möglichkeit einer Wiederaufnahme abgesehen, bestehen aber auch für die betroffenen Unternehmen erhebliche Anreize dafür, bei drohenden Maßnahmen der Wettbewerbsbehörde Verpflichtungszusagen abzugeben. Das ergibt sich schon daraus, dass solche Verfahren auch Ressourcen der von ihnen betroffenen Unternehmen binden und ihr rechtsförmlicher Abschluss ggf. mit Reputationsverlusten verbunden ist. Hinzu kommt, dass die Unternehmen bei Verpflichtungszusagen Einfluss darauf behalten, auf welche Weise die nach Auffassung der Wettbewerbsbehörde bestehenden Wettbewerbsgefahren beseitigt werden. Darüber hinaus kommt einer Entscheidung der Wettbewerbsbehörde, mit der diese die angebotenen Verhaltenszusagen für verbindlich erklärt, keine Bindungswirkung für zivilrechtliche Auseinandersetzungen zu.[239] Sie enthält insbesondere keine Feststellung eines wettbewerbsrechtswidrigen Verhaltens.[240]

Sollte es im Bereich des „Trusted Computing“ zu Ermittlungen der Wettbewerbsbehörden kommen, die voraussichtlich in eine förmliche Abhilfemaßnahme führen werden, erschiene daher die Verfahrensbeilegung durch entsprechende Verhaltenszusagen als praktisch sinnvolle Alternative. Voraussetzung hierfür ist indes insbesondere die Bereitschaft des betreffenden Unternehmens, eine solche Zusage abzugeben und sein Verhalten entsprechend zu ändern.

---

236 Bechtold (Fn. 184), § 32b Rn. 4.
237 Bechtold (Fn. 184), § 32b Rn. 4; Bechtold/Bosch/Brinker/Hirsbrunner (Fn. 185), Art. 9 VO 1/2003 Rn. 9.
238 Diese Möglichkeit besteht, wenn sich die tatsächlichen Verhältnisse in einem wesentlichen Punkt nachträglich geändert haben, wenn die beteiligten Unternehmen ihre Verpflichtungen nicht einhalten oder wenn die ursprüngliche Entscheidung auf unvollständigen, unrichtigen oder irreführenden Angaben der Parteien beruhte, § 32b Abs. 2 GWB, Art. 9 Abs. 2 der Wettbewerbsverordnung 1/2003.
239 Bechtold (Fn. 184), § 32b Rn. 5.
240 Bechtold (Fn. 184), § 32b Rn. 5.

8.2.1.3 Zwischenergebnis

Die Verhinderung von Wettbewerbsgefahren ist zuvörderst die Aufgabe des Wettbewerbsrechts selbst. Dessen unmittelbare Steuerungswirkung kann über den Erlass von Leitlinien und Auslegungshinweisen durch die zuständigen Wettbewerbsbehörden erheblich gesteigert werden. Das gilt gerade auch angesichts der wettbewerbsrechtlichen Risiken, die im Falle von „Trusted Computing“ einen erheblichen Komplexitätsgrad aufweisen.

Wo die Steuerungswirkung des Wettbewerbsrechts alleine nicht ausreicht, kann es erforderlich werden, dass die zuständige Wettbewerbsbehörde zum Schutz des Wettbewerbs ein entsprechendes Verfahren einleitet. Ermittlungsmaßnahmen im Rahmen eines solchen Verfahrens setzen voraus, dass tatsächliche Umstände auf eine Verletzung des Wettbewerbsrechts hindeuten. In Betracht kommen aber auch Enqueteuntersuchungen eines ganzen Wirtschaftsbereiches, die bereits dann möglich sind, wenn bestimmte Umstände vermuten lassen, dass der Wettbewerb möglicherweise beschränkt ist.

Im Rahmen eines konkreten Kartell- oder Missbrauchsverfahrens können noch vor Verfahrensabschluss einstweilige Maßnahmen getroffen werden. Solche Maßnahmen werden im Falle von „Trusted Computing“ jedoch voraussichtlich nur ausnahmsweise in Betracht kommen. Grund hierfür ist gerade die Komplexität der dort zu erwartenden Fragen. Diese wird einer frühzeitigen Substantiierung entsprechender wettbewerbsrechtlicher Bedenken oftmals entgegenstehen. Diese Komplexität hat auch zur Folge, dass endgültige Abhilfemaßnahmen in aller Regel erst nach Abschluss langjähriger Ermittlungsverfahren ergehen können. Dies deckt sich mit den Erfahrungen aus der wettbewerbsrechtlichen Praxis und wirft die generelle Frage nach der Wirksamkeit des allgemeinen Wettbewerbsrechts in IT-Märkten auf. Sollte es im Bereich des „Trusted Computing“ zu Ermittlungen der Wettbewerbsbehörden kommen, erscheint vor diesem Hintergrund eine möglichst frühzeitige Verfahrensbeilegung durch entsprechende Verhaltenszusagen als praktisch sinnvolle Alternative. Voraussetzung hierfür ist indes eine entsprechende Kooperationsbereitschaft des betreffenden Unternehmens.

8.2.2 Informationspolitik

Neben dem Wettbewerbsrecht stehen dem Staat aber auch andere Handlungsoptionen zur Verfügung, mit denen er ohne vorherige gesetzgeberische Maßnahmen auf wettbewerbspolitische (und ggf. auch sonstige) Risiken des „Trusted Computing“ reagieren und auf die Umsetzung seiner diesbezüglichen Gestaltungsvorstellungen hinwirken kann. Zu denken wäre insoweit zunächst etwa an eine staatliche Informationspolitik. Hier hat die Rechtsprechung des Bundesverfassungsgerichts in den letzten Jahren die Möglichkeiten und Grenzen aufgezeigt, die für staatliches Informationshandeln jenseits spezieller gesetzlicher Ermächtigungsgrundlagen bestehen.

8.2.2.1 Formelle Anforderungen

In formeller Hinsicht setzt die Verbreitung staatlicher Informationen eine Aufgabe der handelnden Stelle voraus,[241] zu deren Erreichung das staatliche Informationshandeln beitragen kann. Erforderlich ist ferner die Einhaltung der Zuständigkeitsgrenzen.[242]

8.2.2.1.1 Aufgabe der staatlichen Stelle

Da das Bundeskartellamt grundsätzlich nur die Aufgabe hat, reaktiv Verletzungen des Kartell- und Missbrauchsverbotes abzustellen, dürfte eine präventive Informationspolitik schon aus diesem Grund nicht zu seinen Aufgaben gehören. Demgegenüber gehört es zu den Aufgaben der Regierung, die Öffentlichkeit über wichtige Vorgänge auch außerhalb oder weit im Vorfeld ihrer eigenen gestaltenden politischen Tätigkeit zu unterrichten.[243] Dieser Aufgabe kommt u. a. dann besondere Bedeutung zu, wenn die Informationsversorgung der Bevölkerung auf interessengeleiteten, mit dem Risiko der Einseitigkeit verbundenen Informationen beruht und die gesellschaftlichen Kräfte nicht ausreichen, um ein hinreichendes Informationsgleichgewicht herzustellen.[244] Gerade wenn zeitnahes Handeln geboten ist, kann die Regierung nicht darauf verwiesen werden, sich auf Gesetzesinitiativen zu beschränken oder auf administrative Maßnahmen anderer staatlicher Stellen zu warten.[245] Vielmehr gehört es dann auch zu den Aufgaben der Regierung, den Bürgern durch Aufklärung, Beratung und Verhaltensempfehlungen Orientierung zu geben.[246]

Inwieweit die Information der Öffentlichkeit im Fall von „Trusted Computing“ zu den Aufgaben der Regierung gehört, wird vor diesem Hintergrund entscheidend von der Art des zu erwartenden Problems und des Einflusses abhängen, den der einzelne Bürger auf die Bewältigung dieses Problems hat. Angesichts der erheblichen gesamtgesellschaftlichen Bedeutung der IT-Branche dürfte dabei die Information über solche Wettbewerbsgefahren zur Aufgabe der Regierung gehören, durch welche die Marktbedingungen nicht nur singulär und unerheblich beeinflusst werden.

Sobald erst einmal die im IT-Bereich allgegenwärtigen Netzeffekte in nennenswertem Umfang greifen, sind wettbewerbliche Fehlentwicklungen, wenn überhaupt, nur noch

---

241 BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 50 (Juris) – Frostschutzwein.
242 BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 670/91, Rn. 83 (Juris) – Psychosekte; Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 50 (Juris) – Frostschutzwein.
243 BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 670/91, Rn. 74 (Juris) – Psychosekte; Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 53 (Juris) – Frostschutzwein; BVerwG, Urt. v. 15.12.2005 – Az. 7 C 20.04, Rn. 27 (Juris) – Scientology.
244 BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 670/91, Rn. 74 (Juris) – Psychosekte; Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 53 (Juris)– Frostschutzwein.
245 BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 54 (Juris) – Frostschutzwein.
246 BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 670/91, Rn. 75 (Juris) – Psychosekte; Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 54 (Juris) – Frostschutzwein; BVerwG, Urt. v. 15.12.2005 – Az. 7 C 20.04, Rn. 27 (Juris) – Scientology.

durch massive Eingriffe in das Marktgeschehen zu korrigieren. Deshalb wird insoweit auch regelmäßig zeitnahes Handeln geboten sein, das nicht zugunsten späterer Maßnahmen etwa der Wettbewerbsbehörden zurückgestellt werden müsste. Der Einfluss des einzelnen Bürgers wird sich dabei i. d. R. aus seiner Konsumentscheidung ergeben, sofern er diese von ihren wettbewerbspolitischen Informationen (mit-) abhängig macht. Damit kann die Information über Wettbewerbsgefahren im Bereich des „Trusted Computing“ grundsätzlich zur Aufgabe der Regierung gehören.

Im Prinzip könnten auch Gefahren für andere öffentliche Interessen eine staatliche Informationspolitik im Bereich des „Trusted Computing“ nahelegen. Das betrifft erneut etwa das Recht auf informationelle Selbstbestimmung oder sicherheitspolitische Interessen der Bundesrepublik Deutschland. Gerade mit Blick auf das Recht auf informationelle Selbstbestimmung bestehen mit den Datenschutzbeauftragten des Bundes und der Länder allerdings bereits staatliche Stellen, die ihren Schutzauftrag gerade auch durch die Information der Öffentlichkeit wahrnehmen. Hinzu kommt die Informationsbereitstellung durch eher technikorientierte Behörden wie das Bundesamt für Sicherheit in der Informationstechnik und eine generell hohe öffentliche Aufmerksamkeit gegenüber Bedrohungen der informationellen Selbstbestimmung. Damit dürfte insoweit kein Informationsdefizit drohen, das durch eine Informationspolitik der Regierung kompensiert werden müsste.

8.2.2.1.2 Einhaltung der Zuständigkeitsgrenzen

Auch hinsichtlich der Einhaltung der Zuständigkeitsgrenzen gelten für eine Informationstätigkeit der Bundesregierung einige Besonderheiten. Die Bundesregierung ist überall dort zur Informationsarbeit berechtigt, wo ihr eine gesamtstaatliche Verantwortung[247] der Staatsleitung zukommt, die mit Hilfe von Informationen erfüllt werden kann.[248] Anhaltspunkte für eine solche Verantwortung[249] lassen sich etwa aus sonstigen Kompetenzvorschriften gewinnen, beispielsweise aus den grundgesetzlichen Gesetzgebungskompetenzen.[250] Nach Art. 74 Abs. 1 Nr. 11 GG besitzt der Bund eine (konkurrierende) Gesetzgebungskompetenz für das Recht der Wirtschaft. Dies betrifft

---

247 Eine solche gesamtstaatliche Verantwortung liegt insbesondere vor, wenn Vorgänge überregionalen Charakter haben und eine bundesweite Informationsarbeit der Regierung die Effektivität der Problembewältigung fördert, vgl. BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 670/91, Rn. 84 (Juris) – Psychosekte; Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 56 (Juris) – Frostschutzwein.

248 BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 670/91, Rn. 84 (Juris) – Psychosekte; Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 56 (Juris) – Frostschutzwein; OVG Münster, Beschl. v. 16.2.2004 – Az. 5 A 637/02, Rn. 21 (Juris) – Mun-Bewegung.

249 Die Ermächtigung der Bundesregierung zum Informationshandeln ist zugleich im Verhältnis zu den Ländern eine andere Regelung im Sinne des Art. 30 GG. Maßgebend für die Kompetenz der Bundesregierung im Bereich des Informationshandelns sind somit nicht die Art. 83 ff. GG; die Regierungstätigkeit ist nicht Verwaltung im Verständnis dieser Normen, siehe BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 670/91, Rn. 85 (Juris) – Psychosekte; Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 57 (Juris) – Frostschutzwein.

250 BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 670/91, Rn. 84 (Juris) – Psychosekte; Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 56 (Juris) – Frostschutzwein.

auch rechtliche Bestimmungen zum Schutz des Wettbewerbs im Bereich der Wirtschaft, was gerade auch in den bundesgesetzlichen Regelungen des GWB zum Ausdruck kommt.

Unabhängig von einer etwaigen Zuständigkeit einzelner Behörden[251] ist die Bundesregierung somit grundsätzlich für Informationsarbeit über Wettbewerbsgefahren im Bereich des „Trusted Computing“ zuständig. Sie kann daher einen bestimmten Vorgang aufgreifen, gegenüber der Öffentlichkeit darstellen und bewerten und auch Empfehlungen oder Warnungen aussprechen, soweit sie dies zur Problembewältigung für erforderlich hält.[252] Auf der Ebene der Bundesregierung ergibt sich die weitere Zuständigkeit schließlich aus Art. 65 GG,[253] so dass der Bundesminister für Wirtschaft und Technologie in aller Regel für die staatliche Informationspolitik (der Bundesregierung) in diesem Bereich zuständig sein wird.

8.2.2.2 Materielle Anforderungen

In materieller Hinsicht müssen marktbezogene Informationen, die potentiell Einfluss auf die Erwerbsmöglichkeiten der betroffenen Unternehmen haben, nach der Rechtsprechung des Bundesverfassungsgerichts inhaltlich zutreffend sein,[254] unter Beachtung des Gebots der Sachlichkeit[255] sowie mit angemessener Zurückhaltung[256] formuliert werden. Außerdem dürfen sie sich nicht als funktionales Äquivalent eines Grundrechtseingriffs darstellen. Für eine etwaige Informationstätigkeit im Bereich des „Trusted

---

251 Das Informationshandeln der Bundesregierung wird nicht von Regelungen berührt, die Verwaltungsbehörden im Rahmen des Gesetzesvollzugs zur Unterrichtung und Warnung der Öffentlichkeit ermächtigen, siehe BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 670/91, Rn. 86 (Juris) – Psychosekte; Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 68 (Juris) – Frostschutzwein. Die elementare Bedeutung vollständiger Information rechtfertigt eine Unterrichtung durch die Bundesregierung, die ggf. auch die Kompetenzen anderer Staatsorgane übergreift, BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 670/91, Rn. 86 (Juris) – Psychosekte; Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 58 (Juris) – Frostschutzwein.

252 Vgl. Beschl. v. 26.6.2002 – Az. 1 BvR 670/91, Rn. 84 (Juris) – Psychosekte; BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 56 (Juris) – Frostschutzwein.

253 BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 670/91, Rn. 83 (Juris) – Psychosekte; Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 55 (Juris) – Frostschutzwein.

254 BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 60 (Juris) – Frostschutzwein.

255 Wertungen sind also nicht generell ausgeschlossen, dürfen aber nicht auf sachfremden Erwägungen beruhen, BVerfG, Beschl. v. 28.7.2004 – Az. 1 BvR 2566/95, DVBl 2005, 106, 107 – gerlach-report; Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 61 (Juris) – Frostschutzwein; OVG Münster, Beschl. v. 16.2.2004 – Az. 5 A 637/02, Rn. 5 (Juris) – Mun-Bewegung. Außerdem darf die Information in der Form weder unsachlich noch herabsetzend formuliert sein, BVerfG, Beschl. v. 28.7.2004 – Az. 1 BvR 2566/95, DVBl 2005, 106, 107 – gerlach-report; Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 61 (Juris) – Frostschutzwein; OVG Münster, Beschl. v. 16.2.2004 – Az. 5 A 637/02, Rn. 33 (Juris) – Mun-Bewegung.

256 Unter Berücksichtigung möglicher nachteiliger Wirkungen auf betroffene Unternehmen ist die staatliche Information im Einzelfall auf das Maß des Erforderlichen zu beschränken, BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 61 (Juris) – Frostschutzwein; OVG Münster, Beschl. v. 16.2.2004 – Az. 5 A 637/02, Rn. 5 (Juris) – Mun-Bewegung.

Computing“ ergeben sich insoweit besondere Beschränkungen durch das Erfordernis inhaltlicher Richtigkeit und durch das Verbot der Eingriffsäquivalenz.[257]

8.2.2.2.1 Inhaltliche Richtigkeit der Information

Schon angesichts der komplexen tatsächlichen Zusammenhänge im Bereich des „Trusted Computing“ wird hinsichtlich etwaigen staatlichen Informationshandelns besondere Zurückhaltung geboten sein. Das dürfte allerdings nicht bedeuten, dass eine Wettbewerbsbeschränkung stets bereits nachgewiesen sein muss. Staatliche Informationspolitik soll schließlich gerade dazu dienen, der Gefährdung öffentlicher Interessen zu einem möglichst frühen Zeitpunkt entgegenzuwirken. Erforderlich ist daher nur eine Sachaufklärung „im Rahmen des Möglichen“.

Auch wenn danach nicht feststeht, dass es tatsächlich zu einer Wettbewerbsbeschränkung kommen wird, könnte deshalb jedenfalls über die Gefahr einer solchen Beschränkung informiert werden, die dabei natürlich auch als bloße Gefahr bezeichnet werden müsste. Im Einzelfall könnte des Weiteren auch die Information über wettbewerbspolitisch unerwünschte Entwicklungen in Betracht kommen, die sich jenseits der wettbewerbsrechtlichen Verbotsnormen bewegen. Dies könnte beispielsweise das Entstehen von Pfadabhängigkeiten durch „Trusted Computing“ betreffen, die bisweilen als wettbewerbspolitische Gefahr identifiziert werden.[258] Gerade dort, wo hierdurch Wettbewerber nicht missbräuchlich behindert werden, sondern nur die Bindung des Endnutzers an ein bestimmtes (Gesamt-) System verstärkt wird, könnte Anlass für staatliches Informationshandeln bestehen.

Nur ausnahmsweise kann die staatliche Stelle darüber hinausgehend zur Veröffentlichung von Informationen auch dann berechtigt sein, wenn die Richtigkeit der Informationen noch nicht abschließend geklärt ist.[259] Eine solche Verdachtsinformation kann erfolgen, wenn eine entsprechende Aufklärung der Marktteilnehmer im öffentlichen Interesse liegt.[260] Dabei muss allerdings grundsätzlich auch über die verbleibenden Unsicherheiten im Hinblick auf die Richtigkeit der Information informiert werden.[261] Außerdem ist der Sachverhalt zumindest im Rahmen des Möglichen sorgsam und unter Nutzung verfügbarer Informationsquellen sowie in dem Bemühen um die nach den Umständen erreichbare Verlässlichkeit aufzuklären.[262]

---

257 Daneben sind natürlich auch die anderen Anforderungen einzuhalten, insbesondere das Diskriminierungsverbot. Mit diesem wäre es insbesondere nicht zu vereinbaren, alleine aufgrund der Herkunft nur vor der Tätigkeit ausländischer Unternehmen zu wahren, deutsche Unternehmen, die an entsprechenden Maßnahmen ebenso beteiligt sind, aber unerwähnt zu lassen.

258 Vgl. Bechtold (Fn. 127), S. 88 f.

259 BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 60 (Juris) – Frostschutzwein.

260 BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 60 (Juris) – Frostschutzwein.

261 BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 60 (Juris) – Frostschutzwein.

262 BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 60 (Juris) – Frostschutzwein.

8.2.2.2.2 Keine Eingriffsäquivalenz

Grenzen werden dem staatlichen Informationshandeln aber vor allem dadurch gezogen, dass es auch in seiner Zielsetzung und seinen Wirkungen nicht Ersatz für eine staatliche Maßnahme sein darf, die als Grundrechtseingriff im herkömmlichen Sinne zu qualifizieren wäre.[263] Unzulässig ist es mithin, zielgerichtet zulasten bestimmter Betroffener einen im öffentlichen Interesse erwünschten Erfolg herbeizuführen.[264] Staatliche Informationspolitik wird daher umso eher rechtswidrig sein, je mehr sie typischem auf den Einzelfall bezogenen Verwaltungshandeln entspricht.[265] Rein faktisch-mittelbare Grundrechtsbeeinträchtigungen sind der Rechtsprechung des Bundesverfassungsgerichts zufolge demgegenüber unschädlich.[266]

Auch dies spricht dafür, dass die staatliche Information über drohende Wettbewerbsgefahren eher im Vorfeld tatsächlicher Wettbewerbsbeschränkungen oder aber jenseits des Anwendungsbereiches der wettbewerbsrechtlichen Verbotsnormen erfolgen darf und, wenn überhaupt, auch nur dort erfolgen sollte. Insoweit ist auch zu berücksichtigen, dass die Rechtsprechung des Bundesverfassungsgerichts zu staatlichem Informationshandeln in der Rechtswissenschaft stark umstritten ist.[267]

Es besteht mithin ein nicht zu vernachlässigendes Risiko, dass diese Rechtsprechung in künftigen Entscheidungen wieder aufgegeben wird, entsprechendes Informationshandeln dann aber ohne gesetzliche Ermächtigung generell verfassungswidrig wäre. Schon dieses Risiko wie auch die mit erheblichen Einschätzungsunsicherheiten verbundenen Voraussetzungen staatlichen Informationshandelns lassen es empfehlenswert erscheinen, die Möglichkeit einer entsprechenden Informationstätigkeit insgesamt nur unter größter Zurückhaltung in Betracht zu ziehen.

8.2.2.3 Zwischenergebnis

Ein möglichst frühzeitiger Schutz des Wettbewerbs kann jenseits des Wettbewerbsrechts möglicherweise auch durch staatliches Informationshandeln erreicht werden. Maßgeblich ist hierfür die einschlägige Rechtsprechung des Bundesverfassungsgerichts, die allerdings sehr umstritten ist. Auf ihrer Grundlage dürfte eine entsprechende Informationstätigkeit hinsichtlich ernstzunehmender Wettbewerbsgefahren im Zusammenhang mit der „Trusted Computing“-Technologie in den Aufgaben- und Zuständigkeitsbereich der Regierung bzw. des Bundeswirtschaftsministers fallen. Solche Informa-

---

263 BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 670/91, Rn. 76 (Juris) – Psychosekte; Beschl. v. 26.6.2002 – Az. 1 BvR 558/91, 1 BvR 1428/91, Rn. 62 (Juris) – Frostschutzwein.
264 BVerwG, Urt. v. 15.12.2005 – Az. 7 C 20.04, Rn. 29 (Juris) – Scientology.
265 BVerwG, Urt. v. 15.12.2005 – Az. 7 C 20.04, Rn. 30 (Juris) – Scientology.
266 BVerfG, Beschl. v. 26.6.2002 – Az. 1 BvR 670/91, Rn. 76 (Juris) – Psychosekte; BVerwG, Urt. v. 15.12.2005 – Az. 7 C 20.04, Rn. 27 (Juris) – Scientology; OVG Münster, Beschl. v. 16.2.2004 – Az. 5 A 637/02, Rn. 21 (Juris) – Mun-Bewegung.
267 Vgl. etwa Bethge, Jura 2003, 327; Huber, JZ 2003, 290; Ohler, ZLR 2002, 631.

tionen müssen aber inhaltlich zutreffend sein und unter Beachtung des Gebots der Sachlichkeit und mit angemessener Zurückhaltung formuliert werden. Vor allem aber dürfen sie kein funktionales Äquivalent eines Grundrechtseingriffes sein.

Es spricht daher viel dafür, von der Möglichkeit staatlicher Informationstätigkeit im Bereich des „Trusted Computing“, wenn überhaupt, nur sehr zurückhaltend Gebrauch zu machen. Zu denken wäre evtl. noch daran, über drohende Wettbewerbsgefahren im Vorfeld tatsächlicher Wettbewerbsbeschränkungen zu informieren. Auch auf wettbewerbspolitisch unerwünschte Entwicklungen, die außerhalb des Anwendungsbereiches der wettbewerbsrechtlichen Verbotsnormen liegen, könnte staatlicherseits evtl. informiert werden. Das betrifft beispielsweise die volkswirtschaftlichen Konsequenzen weitgehender Pfadabhängigkeiten, die durch „Trusted Computing“ geschaffen bzw. verstärkt werden können.

8.2.3 Beschaffungswesen

Zwischen den Grenzpunkten finaler Eingriffe auf Grundlage des Wettbewerbsrechts und bloßer Informationspolitik nimmt der Staat aber auch rein faktisch als Marktteilnehmer Einfluss auf die Marktverhältnisse. Angesichts der Größe der öffentlichen Verwaltung ist der Staat nämlich ein bedeutsamer Nachfrager nach IT-Produkten und IT-Dienstleistungen.[268] Er kann somit durch seine Nachfrageentscheidung Einfluss auf den Markterfolg bestimmter Anbieter nehmen.[269] Zugleich besteht auf Seiten der Anbieter wegen der erheblichen Bedeutung der staatlichen IT-Beschaffung ein starkes Interesse daran, bei entsprechenden Beschaffungsentscheidungen berücksichtigt zu werden. Der im Rahmen des Beschaffungswesens bestehende Einfluss des Staates kann deshalb auch bereits im Vorfeld konkreter Nachfrageentscheidungen Wirkung zeitigen.

Die rechtlichen Rahmenbedingungen, die bei der Beschaffung von IT-Produkten und IT-Dienstleistungen durch die öffentliche Hand zu beachten sind, richten sich nach dem Wert des jeweiligen Auftragsgegenstandes.[270] In der Vergabeverordnung (VgV) sind Schwellenwerte festgelegt. Von deren Erreichen hängt es ab, ob die vergabrechtlichen Vorgaben des GWB, der VgV und für die Gebietskörperschaften (Bund, Länder, Kommunen) auch der Verdingungsordnung für Leistungen (VOL/A)[271] zur Anwendung kommen oder nicht. Für den IT-Bereich betragen diese Schwellenwerte derzeit i. d. R.

---

268 In der EG beliefen sich die Beschaffungsvolumina der öffentlichen Hand im Jahr 2001 auf etwa 14 % des Bruttoinlandprodukts der Gemeinschaft, siehe Kommission, Interpretierende Mitteilung der Kommission über das auf das Öffentliche Auftragswesen anwendbare Gemeinschaftsrecht und die Möglichkeiten zur Berücksichtigung von Umweltbelangen bei der Vergabe öffentlicher Aufträge, KOM (2001) 274 endgültig, S. 6.

269 Heckmann, CR 2005, 711, 714.

270 § 100 Abs. 1 GWB.

271 § 4 Abs. 1 VgV.

137.000 Euro für Liefer- und Dienstleistungen der obersten oder oberen Bundesbehörden sowie vergleichbarer Bundeseinrichtungen[272] sowie 211.000 Euro für alle anderen Liefer- und Dienstleistungsaufträge[273].

Fraglich ist im vorliegenden Kontext, inwieweit bei der IT-Beschaffung Erwägungen berücksichtigungsfähig sind, die der Durchsetzung politischer Ziele jenseits der möglichst optimalen Bedarfsdeckung dienen. Da bei solchen Maßnahmen der Einfluss auf das Verhalten der Anbieter im Vordergrund steht, kann insoweit von einer marktregulierenden Einflussnahme gesprochen werden.[274]

8.2.3.1 Marktregulierende Einflussnahme ab Erreichen der vergaberechtlichen Schwellenwerte

Auch innerhalb des Vergabeverfahrens nach §§ 97 ff. GWB i. V. m der VgV und der VOL/A bestehen verschiedene Ansatzpunkte, an denen die öffentliche Hand marktregulierenden Einfluss nehmen kann

8.2.3.1.1 Entscheidung über den Auftragsgegenstand

So unterliegt die Entscheidung über den Auftragsgegenstand bereits nicht den rechtlichen Vorgaben für das Vergabeverfahren.[275] Insoweit müssen lediglich die allgemeinen rechtlichen Vorgaben eingehalten werden, insbesondere also das Diskriminierungsverbot[276] und der Grundsatz der Verhältnismäßigkeit.[277] Besondere Anforderungen an den Leistungsgegenstand, mit denen das öffentliche Interesse durchgesetzt werden soll, müssen somit hierzu geeignet, erforderlich und angemessen sein und dürfen vorbehaltlich eines sachlichen Grundes nicht zu Ungleichbehandlungen führen. In diesen Grenzen ist die öffentliche Stelle frei, den Auftragsgegenstand unter Berücksichtigung öffentlicher Interessen zu bestimmen.[278] Da es im IT-Bereich allerdings i. d. R. um den Erwerb von Endprodukten geht, sind einer marktregulierenden Einflussnahme hier enge Grenzen gesetzt.[279]

---

272 § 2 Nr. 2 VgV.
273 § 2 Nr. 3 VgV.
274 Begriff nach Heckmann, CR 2005, 711, 714.
275 Kommission, KOM (2001) 274 endgültig (Fn. 268), S. 8 f.; *Winkler,* KommJur 2007, 330, 331.
276 Kommission, KOM (2001) 566 endgültig, S. 7.
277 Kommission, KOM (2001) 274 endgültig (Fn. 268), S. 9.
278 Kommission, KOM (2001) 566 endgültig, S. 7; KOM (2001) 274 endgültig (Fn. 268), S. 8.
279 Vgl. auch Kommission, KOM (2001) 566 endgültig, S. 7; KOM (2001) 274 endgültig (Fn. 268), S. 9.

8.2.3.1.2 Vergabeverfahren

Marktregulierender Einfluss im Rahmen des Vergabeverfahrens ist denkbar bei der Festlegung der Leistungsanforderungen sowie bei der Festlegung von Eignungs- und Zuschlagskriterien.

8.2.3.1.2.1 Leistungsanforderungen

Die Leistungsanforderungen enthalten mit den technischen Anforderungen objektive, messbare Angaben über den Auftragsgegenstand.[280] Zu ihnen gehören auch Vorgaben für das Produktionsverfahren,[281] soweit sie sich auf das Produkt selbst beziehen, nicht aber nur auf das produzierende Unternehmen.[282] Sofern es im Falle von „Trusted Computing“ um die Durchsetzung öffentlicher Interessen im Bereich der technischen Sicherheit, des Datenschutzes etc. geht, können diese durch die Bezugnahme auf einschlägige Normen vergaberechtliche Wirksamkeit entfalten. Schwieriger verhält es sich indes bei der Durchsetzung wettbewerbspolitischer Belange, da sich die dort drohenden Beeinträchtigungen in aller Regel nicht aus objektiven Eigenschaften der betreffenden Produkte ergeben. Etwas anderes dürfte jedoch dort gelten, wo bestimmte Interoperabilitätsmöglichkeiten bzw. -beschränkungen wettbewerbsrechtlich relevant und objektiv beschreibbar sind, also z. B. die Unterstützung offener Dateiformate durch die zu beschaffende Applikation.

8.2.3.1.2.2 Eignungskriterien

Bei den Eignungskriterien geht es demgegenüber darum, welche Unternehmen sich um einen öffentlichen Beschaffungsauftrag bewerben können. Insoweit kommt es grundsätzlich nur auf die Fachkunde,[283] die Leistungsfähigkeit[284] und die Zuverlässigkeit[285] der Unternehmen an; andere oder weitergehende Anforderungen dürfen an Auftragnehmer nur gestellt werden, wenn dies gesetzlich vorgesehen ist.[286] Insbesondere soweit es um die Fachkunde und um die technische Leistungsfähigkeit geht, sind grundsätzlich Anforderungen denkbar, mit denen etwa die Einhaltung bestimmter daten-

---

280 Kommission, KOM (2001) 274 endgültig (Fn. 268), S. 11.

281 Kommission, KOM (2001) 566 endgültig, S. 9; KOM (2001) 274 endgültig (Fn. 268), S. 12; *Ziekow,* KommJur 2007, 281, 285.

282 Kommission, KOM (2001) 566 endgültig, S. 9; KOM (2001) 274 endgültig (Fn. 268), S. 13.

283 Fachkundig ist ein Bewerber, wenn er Kenntnisse, Erfahrungen und Fertigkeiten besitzt, die für die Ausführung der zu vergebenden Leistungen erforderlich sind, Otting, in: Bechtold (Fn. 184), § 97 Rn. 21.

284 Leistungsfähig ist ein Bewerber, wenn er über das für die fach- und fristgerechte Ausführung notwendige Personal und Gerät verfügt (technische Leistungsfähigkeit) und die Erfüllung seiner (Leistungs-) Verbindlichkeiten erwarten lässt (wirtschaftliche Leistungsfähigkeit), Otting (Fn. 283), § 97 Rn. 22.

285 Die Zuverlässigkeit ist dann gegeben, wenn der Bewerber bisher seinen gesetzlichen Verpflichtungen nachgekommen ist und aufgrund der Erfüllung auch früherer Verträge eine einwandfreie Ausführung einschließlich Gewährleistung erwarten lässt, Otting (Fn. 283), § 97 Rn. 23.

286 § 97 Abs. 4 GWB.

schutzrechtlicher Vorgaben sichergestellt werden kann.[287] Die Berücksichtigung wettbewerbspolitischer Vorgaben dürfte im Rahmen dieser Kriterien jedoch ausscheiden.

Der einzige Ansatzpunkt, um derartige Erwägungen bei der Festlegung der Anbieterkriterien in das Vergabeverfahren einfließen zu lassen, könnte im Bereich der Anforderungen an die Zuverlässigkeit bestehen. Allerdings müssten etwaige Gesetzesverstöße ein gewisses Gewicht besitzen,[288] nachgewiesen bzw. rechtskräftig festgestellt sein[289] und die Zuverlässigkeit des betreffenden Unternehmens *als Bewerber für die zu vergebende Leistung* in Frage stellen.[290] Diese Anforderung begrenzt die Wirksamkeit entsprechender Einflussnahmen aber erheblich, da die Leistung bei IT-Beschaffungsvorgängen oftmals nicht von dem Hersteller, sondern von einem Dritten (Händler, Importeur etc.) erbracht wird. Die im vorliegenden Kontext potentiell relevanten Verstöße gegen das Wettbewerbsrecht werden jedoch i. d. R. der Sphäre der Produzenten zuzuordnen sein und sind damit der vergaberechtlichen Regulierung entzogen.[291]

8.2.3.1.2.3 Zuschlagskriterien

Auch die Zuschlagskriterien, die der Beurteilung eines Angebotes durch den staatlichen Auftraggeber zugrunde gelegt werden, erlauben in gewissen Grenzen die Berücksichtigung öffentlicher Interessen. Gemäß § 97 Abs. 5 GWB wird der Zuschlag „auf das wirtschaftlichste Angebot“ erteilt. Hiermit ist aber nicht allein das preisgünstigste Angebot gemeint.[292] Vielmehr erlaubt es diese Formulierung dem Auftraggeber, ein optimales Preis-Leistungs-Verhältnis zu erzielen.[293] Damit diese Bewertung objektiv und transparent erfolgt, muss der Auftraggeber vorab angeben, welche Kriterien[294] angewendet werden und für den Zuschlag entscheidend sind.[295] Es gibt keinen feststehenden Katalog potentieller Zuschlagskriterien.[296] Die im konkreten Fall festgelegten Kriterien müs-

---

287 Vgl. für marktregulierende Einflussnahmemöglichkeiten im Bereich der Arbeitsmarktpolitik Kommission, KOM (2001) 566 endgültig, S. 10 f. u. 12 f., und des Umweltschutzes Kommission, KOM (2001) 274 endgültig (Fn. 268), S. 17 ff.

288 Gemäß § 7 Nr. 5 lit. c VOL/A muss es sich um eine „schwere Verfehlung“ handeln.

289 Vgl. zu Verstößen gegen sozialrechtliche Bestimmungen Kommission, KOM (2001) 566 endgültig, S. 11 f., und gegen umweltrechtliche Bestimmungen Kommission, KOM (2001) 274 endgültig (Fn. 268), S. 17.

290 Vgl. § 7 Nr. 5 lit. c VOL/A. Siehe auch Ziekow, KommJur 2007, 281, 287.

291 Vgl. für den Bereich der Kinderarbeit auch Ziekow, KommJur 2007, 281, 284.

292 § 25 Nr. 3 S. 2 VOL/A.

293 Kommission, KOM (2001) 274 endgültig (Fn. 268), S. 20.

294 § 25a Nr. 1 (1) S. 1 VOL/A nennt beispielhaft folgende Kriterien: Qualität, Preis, technischer Wert, Ästhetik, Zweckmäßigkeit, Umwelteigenschaften, Betriebskosten, Rentabilität, Kundendienst und technische Hilfe, Lieferzeitpunkt und Lieferungs- oder Ausführungsfrist.

295 § 25a Nr. 1 [2] VOL/A. Siehe auch EuGH, Urt. v. 17.9.2002 – Rs. C-513/99, Slg. 2002, I-7213, 7277 (Rn. 62) – Concordia Bus Finland; Kommission, KOM (2001) 566 endgültig, S. 14; KOM (2001) 274 endgültig (Fn. 268), S. 20.

296 EuGH, Urt. v. 17.9.2002 – Rs. C-513/99, Slg. 2002, I-7213, 7275 (Rn. 54) – Concordia Bus Finland; Kommission, KOM (2001) 566 endgültig, S. 14; KOM (2001) 274 endgültig (Fn. 268), S. 20.

sen durch den Auftragsgegenstand gerechtfertigt sein,[297] also insbesondere mit ihm zusammenhängen.[298]

Bei der Aufstellung der Kriterien ist das Diskriminierungsverbot zu beachten.[299] Darüber hinaus müssen die Kriterien, die angewendet werden, einen wirtschaftlichen Vorteil für den Auftraggeber mit sich bringen.[300] Dabei ist es allerdings nicht erforderlich, dass jedes Zuschlagskriterium notwendigerweise *rein* wirtschaftlicher Art ist.[301] Es ist deshalb nicht ausgeschlossen, auch Aspekte zu berücksichtigen, die sich auf andere öffentliche Interessen beziehen.[302] Diese müssen sich jedoch zumindest auch in wirtschaftlichen Vorteilen für den Auftraggeber niederschlagen, woran allerdings keine allzu hohen Anforderungen zu stellen sind.[303] Darüber hinaus können auch Kosten, die während des Lebenszyklus eines Produktes anfallen und die der Auftraggeber tragen wird, bei der Ermittlung des wirtschaftlich günstigsten Angebotes berücksichtigt werden.[304]

Im Falle von „Trusted Computing“ kann das beispielsweise Interoperabilitätsanforderungen betreffen, wenn durch diese sichergestellt werden kann, dass die öffentliche Stelle vorhandene (oder künftige) IT-Komponenten unter Vermeidung entsprechender Ersatzinvestitionen (weiter-) verwenden kann. Auch könnte die Unterstützung offener Dateiformate als Zuschlagskriterium in Betracht kommen, da hierdurch Pfadabhängigkeiten und damit einhergehende Wechselkosten vermieden werden können.

Aber auch andere öffentliche Interessen, die bei „Trusted Computing“ berührt sein können, sollten im Einzelfall Ausdruck in Zuschlagskriterien finden können. So kann etwa die Einhaltung bestimmter technischer Vorgaben dazu dienen, zusätzliche Investitionen zum Schutz der Vertraulichkeit von Daten oder der Verfügbarkeit von Systemen zu vermeiden, die anderenfalls notwendig würden. Unzulässig ist demgegenüber die Festlegung von Kriterien, die sich lediglich auf externe Kosten beziehen, die nicht der staatliche Auftraggeber zu tragen hat.[305] Die bloße Verhinderung von Wettbewerbsbeschränkungen oder von Gefahren für andere öffentliche Interessen kann daher als solche nicht in Zuschlagskriterien abgebildet werden.

---

297 § 25a Nr. 1 [1] S. 1 VOL/A.

298 EuGH, Urt. v. 17.9.2002 – Rs. C-513/99, Slg. 2002, I-7213, 7276 (Rn. 59) – Concordia Bus Finland; Kommission, KOM (2001) 566 endgültig, S. 14 f.; KOM (2001) 274 endgültig (Fn. 268), S. 20; Ziekow, KommJur 2007, 281, 285 u. 287.

299 EuGH, Urt. v. 17.9.2002 – Rs. C-513/99, Slg. 2002, I-7213, 7277 (Rn. 63) – Concordia Bus Finland; Kommission, KOM (2001) 566 endgültig, S. 14; KOM (2001) 274 endgültig (Fn. 268), S. 20.

300 Kommission, KOM (2001) 566 endgültig, S. 14; KOM (2001) 274 endgültig (Fn. 268), S. 20. Der Auftraggeber darf sich nur von wirtschaftlichen Überlegungen leiten lassen, EuGH, Urt. v. 3.10.2000 – Rs. C-380/98, Slg. 2001, I-8035, Rn. 17 – University of Cambridge; Kommission, KOM (2001) 566 endgültig, S. 14; KOM (2001) 274 endgültig (Fn. 268), S. 20.

301 EuGH, Urt. v. 17.9.2002 – Rs. C-513/99, Slg. 2002, I-7213, 7275 (Rn. 55) – Concordia Bus Finland.

302 Winkler, KommJur 2007, 330, 332; so für Umweltschutzaspekte auch die Kommission, KOM (2001) 274 endgültig (Fn. 268), S. 20.

303 Der EuGH, Urt. v. 17.9.2002 – Rs. C-513/99, Slg. 2002, I-7213, 7279 (Rn. 69) – Concordia Bus Finland, erwähnt dieses Erfordernis noch nicht einmal explizit.

304 Kommission, KOM (2001) 274 endgültig (Fn. 268), S. 22.

305 Kommission, KOM (2001) 274 endgültig (Fn. 268), S. 23. Vgl. auch Ziekow, KommJur 2007, 281, 285.

Unklar ist, ob Zusatzkriterien festgelegt werden können, die sich nicht auf die Wirtschaftlichkeit eines Angebotes beziehen müssen[306] und dann zur Anwendung gelangen, wenn zwei oder mehr wirtschaftlich gleichwertige Angebote vorliegen.[307] Dies würde es erlauben, auch solche öffentlichen Interessen bei Vergabeverfahren zu berücksichtigen, die keine Auswirkungen auf die Wirtschaftlichkeit (aus Sicht des staatlichen Auftraggebers) haben.[308] Da eine solche Berücksichtigung zusätzlicher Kriterien allerdings vergaberechtlich umstritten ist,[309] wäre ein entsprechendes Vorgehen mit nicht unerheblichen rechtlichen Risiken verbunden.

8.2.3.1.3 Bedingungen für die Auftragsausführung

Schließlich können die staatlichen Auftraggeber öffentliche Interessen unter bestimmten Voraussetzungen auch noch durch zusätzliche Bedingungen für die Auftragsausführung durchsetzen.[310] Die Vertragsausführung als solche muss nämlich lediglich mit den allgemeinen Vorschriften und Grundsätzen des geltenden Rechts im Einklang stehen, insbesondere also auch mit dem Diskriminierungsverbot.[311] Das hat namentlich auch zur Folge, dass es auf diesem Wege nicht zu (verdeckten) Leistungsanforderungen, Auswahlkriterien oder Zuschlagskriterien kommen darf.[312]

Diese Möglichkeit, auf die Ausführung des vergebenen Auftrages Einfluss zu nehmen,[313] dürfte indes nur in sehr geringem Maße eine marktregulierende Einflussnahme zur Durchsetzung öffentlicher Interessen im Bereich des „Trusted Computing“ erlauben. Zu denken wäre insoweit vielleicht noch an die Auflage, etwaige „Trusted Computing“-Komponenten deaktiviert auszuliefern.[314] Auch könnte auf diese Weise verlangt werden, dass „Trusted Computing“-spezifische Betriebssystemerweiterungen, zu denen es alternative Programme von Seiten anderer Anbieter gibt, bei der Auslieferung des beschafften Betriebssystems nicht als voreingestellte Lösungen vorgegeben werden.

---

306 Vgl. hierzu mit Blick auf die Rechtslage vor der Reform des Vergabrechts durch die Koordinierungsrichtlinie 2004/18/EG, ABl. EU 2004 L 134, 114: EuGH, Urt. v. 20.9.1988 – Rs. 31/87, Slg. 1988, 4635, 4657 u. 4659 (Rn. 20 u. 28) – Gebroeders Beentjes; Kommission, KOM (2001) 566 endgültig, S. 16; KOM (2001) 274 endgültig (Fn. 268), S. 23.

307 Kommission, KOM (2001) 566 endgültig, S. 17; KOM (2001) 274 endgültig (Fn. 268), S. 23.

308 Vgl. für arbeitsmarktpolitische Aspekte EuGH, Urt. v. 20.9.1988 – Rs. 31/87, Slg. 1988, 4635, 4659 (Rn. 28 ff.) – Gebroeders Beentjes; für soziale Bedingungen Kommission, KOM (2001) 566 endgültig, S. 17; für Umweltschutzaspekte Kommission, KOM (2001) 274 endgültig (Fn. 268), S. 24.

309 Vgl. etwa Winkler, KommJur 2007, 330, 331, m. w. N., auch zur a. A.

310 Im deutschen Vergaberecht kann dies über § 9 Nr. 3 Abs. 2 VOL/A geschehen, vgl. Ziekow, KommJur 2007, 281, 287.

311 Kommission, KOM (2001) 566 endgültig, S. 18; KOM (2001) 274 endgültig (Fn. 268), S. 25; Winkler, KommJur 2007, 330, 334.

312 Kommission, KOM (2001) 566 endgültig, S. 18; KOM (2001) 274 endgültig (Fn. 268), S. 25; Ziekow, KommJur 2007, 281, 286.

313 Kommission, KOM (2001) 274 endgültig (Fn. 268), S. 25; Winkler, KommJur 2007, 330, 334.

314 Ziekow, KommJur 2007, 281, 285, verweist außerdem auf die Möglichkeit, auf die Beschaffung erst noch herzustellender Waren Einfluss zu nehmen.

8.2.3.2 Marktregulierende Einflussnahme unterhalb der vergaberechtlichen Schwellenwerte

Ein erheblicher Teil der öffentlichen Beschaffungsvorhaben findet unterhalb der verordnungsrechtlich festgelegten Schwellenwerte statt. Für diese Verfahren gelten weder die vergaberechtlichen Vorschriften des GWB noch die VgV. Allerdings gelten auch für solche Vergabeverfahren die verfassungs-[315] und gemeinschaftsrechtlich fundierten Grundsätze der Gleichbehandlung bzw. Nichtdiskriminierung und – hiermit eng verbunden – der Transparenz,[316] die damit einer marktregulierenden Einflussnahme Grenzen setzen.[317] Außerdem ist das Haushaltsrecht der jeweils betroffenen Körperschaft (Bund oder Länder) zu beachten.[318] Das betrifft insbesondere die Grundsätze der Wirtschaftlichkeit und Sparsamkeit.[319]

Darüber hinaus können Verwaltungsvorschriften das Vergabeverfahren unterhalb der Schwellenwerte weiter ausgestalten.[320] Das hat zur Folge, dass oftmals die Verdingungsordnungen auch für unterschwellige Vergabeverfahren zu beachten sind, da deren Geltung verbreitet von der jeweils vorgesetzten Dienstbehörde festgesetzt wird.[321] Zwar sind hier i. d. R. nur die sog. Basisparagraphen der VOL/A einschlägig.[322] Dies führt im vorliegenden Kontext aber im Wesentlichen nur zu gewissen Erleichterungen bei der Festlegung der Leistungsbeschreibung. Vor allem bleibt es bei der Wirtschaftlichkeit eines Angebotes als für den Zuschlag maßgeblichen Gesichtspunkt.[323] Es kann insoweit mithin praktisch uneingeschränkt auf die vorstehenden Ausführungen zu den Einflussnahmemöglichkeiten im Vergabeverfahren nach §§ 97 ff. GWB Bezug genommen werden.

8.2.3.3 Zwischenergebnis

Konkret marktregulierenden Einfluss kann der Staat auch im Rahmen seiner Beschaffungstätigkeit nehmen. Dieser kann indes nur punktuelle Steuerungswirkung entfalten, da insoweit umfassende rechtliche Vorgaben bestehen, die den Beschaffungsvorgang grundsätzlich an reinen Wirtschaftlichkeitserwägungen ausrichten. Das staatliche Beschaffungswesen wird daher nicht geeignet sein, grundlegende wettbewerbliche Fehl-

---

315 Es ist allerdings nicht ganz unumstritten, inwieweit der Gleichbehandlungsgrundsatz aus Art. 3 Abs. 1 GG bei unterschwelligen Bedarfsdeckungsgeschäften anwendbar ist, dafür etwa Otting (Fn. 283), § 97 Rn. 13 u. § 100 Rn. 6.
316 Otting (Fn. 283), § 97 Rn. 2 u. § 100 Rn. 6.
317 Kommission, KOM (2001) 566 endgültig, S. 20; KOM (2001) 274 endgültig (Fn. 268), S. 9 u. 26; Ziekow, KommJur 2007, 281, 287.
318 Vgl. Otting (Fn. 283), § 100 Rn. 9.
319 Otting (Fn. 283), § 100 Rn. 9.
320 Otting ebd.
321 Vgl. Otting (Fn. 283), § 100 Rn. 9.
322 Die sog. „a-Paragraphen" gelten demgegenüber zumindest i. d. R. nur für Vergabeverfahren, bei denen die Schwellenwerte des § 100 Abs. 1 GWB i. V. m. § 2 VgV erreicht werden.
323 § 25 Nr. 3 S. 1 VOL/A.

entwicklungen zu korrigieren. Es kann allerdings dazu beitragen, der Verwirklichung einzelner wettbewerbspolitischer Risiken entgegenzuwirken. Insoweit ist auch die von entsprechenden Anforderungen ausgehende Signalwirkung zu berücksichtigen.

Angesichts der potentiellen Wettbewerbsgefahren im Bereich des „Trusted Computing“ ließe sich vor allem daran denken, bestimmte Interoperabilitätsanforderungen als Leistungsanforderungen für die zu beschaffenden IT-Produkte vorzugeben. Entsprechende Anforderungen an die Interoperabilität und die Unterstützung offener Dateiformate könnten aber auch im Rahmen von Zuschlagskriterien Berücksichtigung finden, da sie i. d. R. auch mit wirtschaftlichen Vorteilen für den staatlichen Auftraggeber verbunden sein werden. Schlussendlich könnte auch durch Vorgaben für die Ausführung des Beschaffungsauftrages auf einzelne wettbewerbspolitische Risiken des „Trusted Computing“ reagiert werden. So könnte z. B. sichergestellt werden, dass etwaige „Trusted Computing“-Komponenten deaktiviert ausgeliefert werden. Auch könnte auf diese Weise verlangt werden, dass „Trusted Computing“-spezifische Betriebssystemerweiterungen, zu denen es alternative Programme von Seiten anderer Anbieter gibt, bei der Auslieferung des beschafften Betriebssystems nicht als voreingestellte Lösungen vorgegeben werden.

8.2.4 Schaffung einer zivilrechtlichen Rahmenregelung

Jenseits der eigentlichen Frage staatlicher Reaktionsmöglichkeiten auf wettbewerbspolitische Risiken des „Trusted Computing“ sind schließlich Maßnahmen denkbar, mit denen Rahmenbedingungen für die Nutzung dieser Technologie gesetzt werden könnten. Bislang steht eine kommerzielle Nutzung von „Trusted Computing“-Lösungen im Massenmarkt noch aus. Ein Grund hierfür könnte darin liegen, dass für die Nutzer derzeit unmittelbare Vorteile entsprechender Anwendungen nicht klar erkennbar sind.[324]

Insoweit wäre zu erwägen, ob durch gesetzgeberische Begleitmaßnahmen potentielle Vorteile von „Trusted Computing“-Anwendungen zumindest in bestimmten Aspekten deutlicher zum Ausdruck gebracht werden. Dies beträfe insbesondere die Nutzung dieser Technologie für Zwecke des elektronischen Geschäftsverkehrs. Man könnte versuchen, noch fehlendes Vertrauen in die vertrauenswürdigen Systemumgebungen durch eine gesetzliche Haftungsregel zu schaffen, die das Risiko einer fehlerhaften Zertifizierung zumindest prima facie dem Anbieter entsprechender Zertifizierungsdienstleistungen zuweist.[325] Vorbild hierfür könnte § 11 des Signaturgesetzes (SigG) sein.[326]

---

324 Neumann (Fn. 127), S. 208 f.

325 Entsprechendes wäre auch denkbar für etwaige Geschäftsmodelle, die auf der Zurverfügungstellung von Referenzwerten für die Integritätsmessung beruhen.

326 Gemäß § 11 Abs. 1 S. 1 SigG hat ein Zertifizierungsdiensteanbieter, der die Anforderungen des SigG oder der Signaturverordnung verletzt oder dessen Produkte für qualifizierte elektronische Signaturen oder sonstige technische Sicherungseinrichtungen versagen, einem Dritten den Schaden zu ersetzen,

Bemerkenswerterweise gibt es dennoch bislang keine rechtspolitische Diskussion über die Schaffung eines entsprechenden „Trusted Computing“-Gesetzes.[327] Entsprechende Maßnahmen des Gesetzgebers, die sinnvollerweise schon mit Blick auf die Vermeidung spezifischer Standortnachteile für die deutsche IT-Wirtschaft ohnehin der gemeinschaftsweiten Harmonisierung bedürften, sind vielmehr erheblichen Bedenken ausgesetzt. Gesetzesvorhaben, die spezifisch der Marktdurchsetzung von „Trusted Computing“-Lösungen dienen sollten, würden einseitig eine ganz bestimmte Technologie fördern. Entsprechende Festlegungen sind zwar nicht ausgeschlossen, erfolgen aber zumeist auf untergesetzlicher Ebene auf Grundlage eines technologieneutralen Rechtsrahmens, der für die Berücksichtigung alternativer Lösungen offen ist.[328] Auch im Bereich der elektronischen Signatur werden auf gesetzlicher Ebene nur allgemeine Anforderungen an Produkte für qualifizierte elektronische Signaturen formuliert,[329] die durch unterschiedliche technische Lösungen umgesetzt werden können.

Gerade mit Blick auf die ohnehin vereinheitlich wirkenden Netzexternalitäten wäre es kaum zu rechtfertigen, ausgerechnet im Bereich des „Trusted Computing“ die Herausbildung technischer Alternativlösungen auch noch durch eine gesetzgeberische Festlegung auf einen bestimmten Standard weiter zu behindern. Von vornherein dürften gesetzgeberische Begleitmaßnahmen daher nur in Betracht kommen, wenn sie einen technologieneutralen Ansatz verfolgen. Dann wäre es aber erforderlich, die Rolle von Zertifizierungsinstanzen in vertrauenswürdigen Systemumgebungen abstrakt zu umschreiben, etwa als Anbieter elektronischer Systemzustandsatteste.

Unabhängig davon, ob ein solcher technologieneutraler Ansatz oder ein „Trusted Computing“-spezifischer Ansatz gewählt würde, sind gesetzgeberische Begleitmaßnahmen aber auch weiteren Bedenken ausgesetzt. Gerade das Beispiel der elektronischen Signatur zeigt, dass trotz einer proaktiven Begleitung durch den Gesetz- und Verordnungsgeber, umfassender Unterstützung durch die öffentliche Verwaltung und intensiver rechtswissenschaftlicher Diskussion die elektronische Signatur auch zehn Jahre nach Inkrafttreten des ersten Signaturgesetzes im Massenmarkt nach wie vor praktisch keine Rolle spielt.[330] Diesem geringen Nutzen stehen erhebliche Kosten gegenüber.

---

den dieser dadurch erleidet, dass er auf die Angaben in einem qualifizierten Zertifikat, einem qualifizierten Zeitstempel oder einer Auskunft über die Zuordnung eines qualifizierten Zertifikates vertraut. Die Ersatzpflicht tritt nicht ein, wenn der Dritte die Fehlerhaftigkeit der Angabe kannte oder kennen musste (§ 11 Abs. 1 S. 2 SigG) und wenn der Zertifizierungsdiensteanbieter nicht schuldhaft gehandelt hat (§ 11 Abs. 2 SigG).

327 Der rechtswissenschaftlichen und rechtspolitischen Literatur sind entsprechende Forderungen, soweit ersichtlich, nicht zu entnehmen. Auch in den studienbegleitenden Gesprächen wurde der Wunsch nach solchen gesetzgeberischen Maßnahmen nicht artikuliert.

328 Vgl. etwa die Möglichkeit von Harmonisierungsmaßnahmen der Kommission im Bereich der Interoperabilität digitaler interaktiver Fernsehdienste nach Art. 18 Abs. 4 S. 2 der Rahmenrichtlinie 2002/21/EG, ABl. EG 2002 L 108, 33.

329 § 17 Abs. 1 SigG.

330 Vgl. schon Koenig/Loetz/Neumann, in: Klumpp/Kubicek/Roßnagel, next generation information society?, 2003, S. 403, 404.

Das betrifft insbesondere auch Kosten der öffentlichen Hand, die neben den genannten Gesetzgebungs- und Förderungsmaßnahmen auch entsprechende institutionelle Rahmenbedingungen geschaffen hat, etwa durch die Einrichtung spezifischer Referate bei der Bundesnetzagentur und durch die Vorhaltung zusätzlicher Ressourcen beim Bundesamt für Sicherheit in der Informationstechnik.

Diesen hohen Kosten steht ein sehr unsicherer Nutzen gegenüber. So ist schon fraglich, ob sich eine sachgerechte Verteilung der Haftungsrisiken nicht auch auf Grundlage der allgemeinen zivilrechtlichen Vorschriften ergeben würde. Diese sind generell geeignet, die Chancen und Risiken, die der Einsatz von „Trusted Computing“ mit sich bringt, in allgemeinen Kategorien wie Sorgfaltsanforderungen und Verkehrspflichten abzubilden und so systemgerecht in den bestehenden Rechtsrahmen einzufügen.[331] Es spricht einiges dafür, dass zwischen dem Anbieter eines Zertifizierungsdienstes und den Nutzern dieses Dienstes ein Schuldverhältnis besteht,[332] innerhalb dessen der Anbieter ohnehin für Pflichtverletzungen zu haften hätte.[333] Insoweit wäre der Anbieter schon auf Grund der allgemeinen Vorschriften wie nach § 11 SigG grundsätzlich zum Beweis verpflichtet,[334] dass er die Pflichtverletzung nicht zu vertreten hat.[335] Diese Änderung der Rechtslage nach Inkrafttreten des SigG[336] würde den Sinn entsprechender Haftungsregeln auf die Klarstellung einer haftungsbegründenden Sonderverbindung beschränken, die sich aber durchaus auch unter Rückgriff auf allgemeine zivilrechtliche Grundsätze annehmen lässt.[337]

Auch insoweit ist überdies daran zu erinnern, dass die Schaffung spezieller Vorschriften durchaus nicht per se mit dem davon erhofften Gewinn an Rechtssicherheit einhergeht. Vielmehr werfen neue rechtliche Regelungen stets auch neue Rechtsfragen auf, die erst durch die Rechtsprechung beantwortet müssen. Das betrifft u. a. das Verhältnis zu den bestehenden gesetzlichen Rahmenbedingungen und umfasst regelmäßig auch die Frage, ob bestimmte Regelungen nicht restriktiv ausgelegt werden müssen.

Im konkreten Fall würde sich auch die Frage nach dem Verhältnis einer neuen Haftungsregelung zum Recht der elektronischen Signatur stellen: Da „Trusted Computing“ auch in entsprechenden Signaturkomponenten eingesetzt werden kann,[338] besteht hier eine Schnittmenge potentieller Haftungsrisiken, deren weitere Umhegung durch gesetz-

---

331 Neumann (Fn. 162), S. 222 f. (voraussichtlich).

332 Selbst wenn man nicht von einem Vertragsschluss ausgehen wollte, wäre noch an die Annahme eines außervertraglichen geschäftlichen Kontakts i. S. v. § 311 Abs. 2 Nr. 3 des Bürgerlichen Gesetzbuches (BGB) oder an einen Vertrag (zwischen dem Anbieter und den Plattforminhabern oder Nutzern) mit Schutzwirkung zugunsten Dritter zu denken.

333 § 280 Abs. 1 S. 1 BGB.

334 Heinrichs, in: Palandt, BGB, 66. A., 2007, § 280 Rn. 34 u. 40.

335 § 280 Abs. 1 S. 2 BGB.

336 Vgl. Heinrichs (Fn. 334), § 280 Rn. 34.

337 Siehe hierzu in und bei Fn. 211. Der Gesetzgeber selbst ging davon aus, dass § 11 SigG in erster Linie eine entsprechende Klarstellung angesichts bestehender Meinungsstreitigkeiten herbeiführen sollte, vgl. Begründung zum Gesetzentwurf der Bundesregierung, BT-Drs. 14/4662, 14, 24 [zu § 11].

338 Bechtold, CR 2005, 393, 404; Neumann (Fn. 162), S. 226 f. (voraussichtlich).

liche Sonderregime zu neuer Rechtsunsicherheiten und auch zur partiellen Entwertung der signaturrechtlichen Bestimmungen führen kann.

Jedenfalls sofern kein hinreichend klar erkennbarer Bedarf für gesetzgeberische Maßnahmen besteht, sollte somit eine entsprechende Steigerung der Regelungskomplexität durch die Schaffung neuer gesetzlicher Bestimmungen nur mit äußerstem Bedacht erwogen werden. Vor diesem Hintergrund spricht wenig für die Schaffung einer gesetzlichen Haftungsregel für verletztes Vertrauen in vertrauenswürdige Systemumgebungen. Dieser Befund wird durch die signaturrechtliche Praxis bestätigt. Die dort in § 11 SigG vorgesehene Regelung spielt, soweit ersichtlich, in der Rechtspraxis bislang überhaupt keine Rolle.[339]

8.3 Handlungsempfehlung

Legt man die Befragung der Marktteilnehmer im Rahmen der vorliegenden Studie zugrunde, scheint kein Anlass für wettbewerbspolitische Handlungsempfehlungen im Bereich des „Trusted Computing“ zu bestehen. Letzten Endes sprechen zwei Erwägungen dafür, diesem Bereich dennoch staatlicherseits weiterhin erhöhte wettbewerbspolitische Aufmerksamkeit zukommen zu lassen. Zum einen kann das Fehlen diesbezüglicher Bedenken auf Seiten der Marktteilnehmer schlichtweg auch auf fehlendes Problembewusstsein hindeuten. Dann wäre die staatliche Sorge um einen unbeschränkten Wettbewerb aber umso dringender geboten.[340] Und zum anderen wögen die Konsequenzen schwer, sollten sich entsprechende Wettbewerbsgefahren dann doch realisieren. Gerade wenn es sich bei „Trusted Computing“ um eine Schlüsseltechnologie handeln sollte, wäre es aus volkswirtschaftlicher Sicht nicht hinnehmbar, wäre der Wettbewerb in den entsprechenden Wachstumsmärkten schon von Anfang an mit Beschränkungen belastet.

Ziel aller wettbewerbspolitischen Maßnahmen sollte es deshalb sein, den Marktteilnehmern die entsprechenden Anreize und Möglichkeiten zu geben, um bereits das Entstehen von Wettbewerbsbeschränkungen weitestmöglich zu verhindern. Soweit es bereits zu solchen Beschränkungen gekommen ist, erscheint demgegenüber ein differenziertes Vorgehen sinnvoll: Dass die grundlegenden Systementscheidungen in der Gründungsphase der TCPA/TCG durch eine kleine Anzahl marktstarker Unternehmen getroffen wurden, lässt sich nicht mehr rückgängig machen, will man nicht die gesamte Technologie in Frage stellen. Demgegenüber dauert die Diskriminierung kleiner und mittlerer Unternehmen durch die Ausgestaltung der Bedingungen für eine Mitgliedschaft in der

---

339 Die Rechtsprechungsdatenbank Juris weist zu § 11 SigG keine Entscheidungen nach. In vereinzelten Entscheidungen, in denen auf diese Vorschrift Bezug genommen wird, geht es nicht um die Anwendung der dort geregelten Haftungsbestimmung, vgl. FG Münster, Urt. v. 23.3.2006 – Az. 11 K 990/05 F, Rn. 79 (Juris).

340 Im Ansatz ähnlich auch Bechtold (Fn. 127), S. 95.

TCG nach wie vor an. Sie beeinträchtigt deren Wettbewerbsmöglichkeiten insbesondere auch im nun bevorstehenden Übergang von der Entwicklungs- in die Anwendungsphase. Gerade angesichts der ohnehin in den IT-Märkten bestehenden Konzentrationstendenzen wäre eine solche Belastung der mittelständischen IT-Wirtschaft im Bereich einer potentiellen Schlüsseltechnologie nicht hinnehmbar.

In den ersten Jahren der TCG führte aus wettbewerbspolitischer Sicht die Ausgestaltung der Mitgliedschaft zu einer Diskriminierung kleiner und mittlerer Unternehmen. Seither wurden die Mitgliedsbeiträge jedoch deutlich gesenkt und dadurch das Diskriminierungspotenzial abgebaut. Für einen Jahresbeitrag von 16.500 US$ kann heute jedes KMU innerhalb der TCG den „Contributor"-Status einnehmen und an den entsprechenden Arbeitsgruppen teilnehmen. Zudem könnten KMU durch ein stärkeres Engagement der Verbände in den entsprechenden Gremien besser repräsentiert werden. Nicht zuletzt das Engagement des BSI innerhalb der TCG bildet eine gewisse Garantie dafür, dass die freien Entwickler sowie deutsche Firmen Zugang zu den Ergebnissen und dem Know-how der TCG haben.

Für die Vermeidung künftiger Wettbewerbsbeschränkungen empfiehlt es sich, die Offenhaltung der Märkte proaktiv zu fördern. Dies kann durch den kombinierten Einsatz verschiedener Steuerungsinstrumente erreicht werden:

1. Die Wettbewerbsbehörden sollten zeitnah Leitlinien und Auslegungshinweise zu den relevanten wettbewerbsrechtlichen Aspekten veröffentlichen. Dabei könnten durchaus primär allgemeine Fragestellungen der Anwendung des Wettbewerbsrechts in den IT-Märkten angesprochen werden, da sich diese letzten Endes auch in den potentiellen Wettbewerbsgefahren für die „Trusted Computing"-Märkte widerspiegeln. Inhaltlich könnte im Rahmen solcher Leitlinien und Hinweise die bisherige Entscheidungspraxis systematisch aufbereitet und weiterentwickelt werden. Besonders dringlich erscheinen darüber hinaus wettbewerbsbehördliche Fingerzeige für die Ausgestaltung von Lizenbedingungen in IT-Märkten.

2. Daneben sollte bei der staatlichen IT-Beschaffung verstärkt Wert auf Interoperabilitätsanforderungen und die Unterstützung offener Dateiformate gelegt werden. Da entsprechende Einflussnahmemöglichkeiten nur punktuell bestehen, erscheint es umso wichtiger, übergreifende Grundsätze für die Berücksichtigung derartiger wettbewerbspolitischer Zielsetzungen zu erarbeiten.

3. Unter Umständen könnte auch jenseits der Veröffentlichung von Leitlinien und Auslegungshinweisen durch die Wettbewerbsbehörden staatliche Informationspolitik zu einzelnen Aspekten des „Trusted Computing" angezeigt sein. So hatte die Bundesregierung mit ihrer Stellungnahme zur TCG und zu NGSCB im Jahr 2004 Pionierarbeit geleistet und hierdurch zugleich erheblichen Einfluss auf die öffentliche Diskussion genommen. Gerade angesichts der geringen Bedeutung, die den wettbewerbspolitischen Implikationen offensichtlich derzeit von Seiten der Marktteilnehmer

beigemessen wird, könnte eine Aktualisierung dieser Stellungnahme das entsprechende Problembewusstsein der Öffentlichkeit wieder schärfen.

Sollten sich trotz entsprechender Maßnahmen Anzeichen für eine tatsächliche Wettbewerbsbeschränkung ergeben, wird die unverzügliche Einleitung entsprechender Wettbewerbsverfahren von entscheidender Bedeutung sein. Insoweit sollten schon jetzt die notwendigen Vorbereitungen innerhalb der zuständigen Wettbewerbsbehörden veranlasst werden. Insbesondere sollte geklärt werden, unter welchen Voraussetzungen die Kommission ein derartiges Verfahren durchzuführen gedenkt, und wo es dem Bundeskartellamt überlassen bleiben würde, gegen derartige Wettbewerbsbeschränkungen vorzugehen.

Schlussendlich wäre zu überlegen, ob die Entwicklungen im Bereich des „Trusted Computing“ nicht zum Anlass für grundlegendere Maßnahmen genommen werden. Das betrifft zunächst die Frage, ob angesichts der weithin stabilen Vermachtung nicht auch die IT-Branche beizeiten einer Enqueteuntersuchung unterzogen werden sollte. Gerade die weitgehende Resistenz der TCG gegenüber wettbewerbspolitischen Bedenken und die fundamentale Bedeutung der Standardisierung in den netzgestützten IT-Märkten könnte es darüber hinausgehend sogar sinnvoll erscheinen lassen, explizite gesetzliche Vorgaben für eine entsprechende Verhaltenskoordinierung der Marktteilnehmer bei der Standardisierung zu schaffen.[341]

Angesichts der erheblichen praktischen Relevanz, der vielfältigen Missbrauchspotentiale und der Schwierigkeiten behördlicher oder gerichtlicher Eingriffe im Einzelfall könnte auch die Frage der Zugangsgewährung zu Schnittstelleninformationen und zu gewerblichen Schutzrechten einen angemessenen Interessenausgleich durch den Gesetzgeber nahelegen.

Demgegenüber sind mit Blick auf die Schaffung spezifischer Haftungsregeln für den Bereich des „Trusted Computing“ keine gesetzgeberischen Maßnahmen angezeigt. Die zu erwartenden Kosten eines solchen Sonderregimes stehen in keinem angemessenen Verhältnis zu dem potentiellen Nutzen, der sich hieraus für die Marktteilnehmer ergeben könnte.

---

341 Vgl. hierzu auch Koenig, EWS 11/2006 (Editorial).

9 Szenarien zur Zukunft von Trusted Computing und darauf aufsetzende Handlungsoptionen

Die im Rahmen dieser Studie ausgewerteten Dokumente, die Auswertung der zahreichen Gespräche mit verschiedenen IT-Sicherheitsexperten sowie die Analysen der Vergleichsmärkte legen den Schluss nahe, dass es sich bei der Trusted Computing-Technologie insbesondere in Hinblick auf ihre Anwendung bei Embbeded Systems in der Sicht der allermeisten Akteure um eine Schlüsseltechnologie handelt, die es den Systemherstellern erlaubt, bei der Systementwicklung die gegenwärtigen Komplexitätsschranken und Bedrohungen zu überwinden.

In vielen Geräten mit Rechnerkapazität, aber auch bei Managementprozessen z. B. bei Enterprise Rights Management und insbesondere im Bereich der mobilen Kommunikation, werden wichtige Einsatzfelder für TC gesehen. Diese Sichtweise wird insbesondere von der Herstellerindustrie von Hardware, etwa Chip- und Rechnerherstellern, aber auch von den in Deutschland aktiven TC-Forschungseinrichtungen vertreten. Es können mit ihrer Hilfe Netzwerke, Plattformen, implementierte Systeme und Endgeräte entwickelt werden, die eine sich immer stärker vernetzende industrielle Gesellschaft benötigt, um das erforderliche Vertrauen in alle Formen von Austauschprozessen und Transaktionen herzustellen.[342]

Insbesondere im Bereich der Scientific Community, Teilen der IT-Sicherheitswirtschaft, aber auch bei den Vertretern der Branchenverbände (TeleTrusT) und Teilen der Anwenderindustrien (Automobilindustrie) bestehen daher große Erwartungen an die künftige Marktrelevanz von TC, die sich nicht auf das Härten von Plattformen, sondern auch auf das sichere Gestalten von Ablaufprozessen in Unternehmen oder Verwaltungen erstrecken.

Auf der anderen Seite aber ist nicht zu übersehen, dass es bislang an wirklich sichtbaren oder relevanten industriellen Anwendungen und deren Umsetzung mangelt und niemand präzise Angaben darüber machen kann, in welchen Bereichen sich TC mittel- und langfristig durchsetzen wird. Dies hat zum einen mit dem hohen Maß an Unsicherheit bei den industriellen Akteuren („es muss der Mehrwert demonstriert werden"), zum anderen aber auch mit der Zeitperspektive zu tun, innerhalb derer marktrelevante Entwicklungen erwartet werden („wirklich marktrelevante Entwicklungen benötigen noch mindestens fünf Jahre"). Zwar scheinen die zahlreichen Einwände und kritischen Argumentationen gegen TC etwa in Hinblick auf den Verlust der Nutzungshoheit, den Datenschutz, DRM oder Usability, wie sie zumindest bis 2004 vorgebracht wurden, weitgehend überwunden zu sein, aber scheinbar besteht das Misstrauen gegenüber den marktmächtigen Akteuren der TC-Arena teilweise fort („ohne Microsoft wird TC nicht zu realisieren sein").

---

342 Vgl. Brandl 2007, S. 39.

Vor diesem Hintergrund wird in allen Expertengesprächen der instrumentelle Charakter von TC und die „Janusköpfigkeit“ dieser Technologie unterstrichen. TC ist offenkundig strukturell offen für „gute“ und für „schlechte“ Anwendungen. Dieses Faktum wäre an sich nicht weiter kritisch, da diese Eigenschaft auf viele Technologien zutrifft. Allerdings erschwert sie die Schaffung einer breiten Awareness für die Chancen von TC.

Mitunter werden auch Vergleiche mit der schwierigen Marktpenetration der (qualifizierten) digitalen Signatur gezogen. Hier war Deutschland bereits vor vielen Jahren Vorreiter und trotz der zwischenzeitlichen Anpassung der rechtlichen Rahmenbedingungen können entsprechende Pull-Faktoren am Markt bislang kaum beobachtet werden.

Auch bei TC besteht der Eindruck, dass diese Technologie der massenmarktlichen Verbreitung (weit) vorauseilt. Das Beispiel digitaler Signaturen wird daher öfter bemüht, um zu verdeutlichen, dass technologisch anspruchsvolle Lösungen wie TC in Massenmärkten nicht selten auf enorme Wirtschaftlichkeits- und Akzeptanzbarrieren stoßen können, die einer schnellen Penetration – ohne weitere Unterstützung aus dem politischen und wirtschaftlichen Umfeld (z. B. durch eGoverment- oder eBanking-Anwendungen) – entgegenstehen.

Zusammengefaßt bedeutet dies, dass das hohe Maß an Unsicherheit, welches die TC-Entwicklung in den Jahren begleitet hat, offenkundig auch in den nächsten Jahren fortbestehen wird. Dies muss für alle Akteure und Entscheidungsträger aus dem forscherischen, wirtschaftlichen sowie politischen Umfeld als in hohem Maße unbefriedigend empfunden werden. Auf der einen Seite gilt es zu vermeiden, dass durch ein allzu voreiliges Handeln falsche Schwerpunkte gesetzt sowie wichtige Mittel und Ressourcen fehlalloziert werden, die damit als „sunk“ betrachtet werden müssen. Auf der anderen Seite gilt es ebenso zu verhindern, dass sich Deutschland, wie teilweise schon in der Vergangenheit, als Vorreiter im Besitz einer wichtigen Technologie mit Schlüsselcharakter befindet, deren Sicherheits- und Wirtschaftspotenziale auf Grund einer allzu großen Zögerlichkeit verschenkt und den Unternehmen anderer Ländern zur Vermarktung überlassen werden.

Um diese Unsicherheiten zu reduzieren, werden im Folgenden drei Szenarien entwickelt, die wahrscheinliche oder denkbare Entwicklungspfade beinhalten: Das erste Szenario beinhaltet ein „Trendszenario“, das die höchste Wahrscheinlichkeit des Eintritts besitzt. Das zweite stellt ein eher optimistisches „Wachstumsszenario“ dar. Dieses Szenario besitzt aus Sicht der Autoren die geringste Eintrittswahrscheinlichkeit. Als drittes Szenario wurde ein eher pessimistisches „Stillstand-Szenario“ beschrieben. Manche Elemente dieses Szenarios besitzen ebenfalls eine vergleichsweise hohe Eintrittswahrscheinlichkeit, so dass es keinesfalls überraschend wäre, wenn die tatsächlich eintretende Entwicklung - wenigstens im Zeitraum bis 2013 - einer Mischung aus „Stillstands-Szenario“ und „Trendszenario“ folgen würde.

Für jedes dieser Szenarien werden Handlungsoptionen konzipiert, die möglichst passgenau auf den in der vorangegangenen Analyse skizzierten Entwicklungen und den Einschätzungen der Experten aufsetzen. Als Zeithorizont haben wir die nächsten fünf Jahre bis 2013 gewählt, um nicht allzu tentativ argumentieren zu müssen.

Die an jedes Szenario anschließenden Handlungsoptionen orientieren sich eng an dem jeweilig aufgespannten Entwicklungsrahmen. Sie sind daher nicht spekulativ, sondern bilden realistische Optionen ab. Sie ermöglichen jedem Leser je nach Einschätzung auch eine abweichende Bewertung der skizzierten Entwicklungen. Auf ein eigenständiges Kapitel zu möglichen Handlungsoptionen wird daher im Rahmen dieser Studie verzichtet.

9.1 Trusted Computing: Das Trendszenario (wahrscheinlicher Fall)

Das Trendszenario beinhaltet den aus der Sicht der Autoren wahrscheinlichsten Eintrittsfall. Die Situation ist von widersprüchlichen, manchmal unklaren und zum Teil intransparenten Informationen gekennzeichnet. Es unterstellt, dass die (potenziellen) industriellen Anwender – von wenigen Ausnahmen abgesehen - geringe Initiative bei der Entwicklung und Implementierung von TC zeigen, sei aus auf Grund der bestehenden Unsicherheiten, sei es aus mangelndem Anwendungsinteresse oder sei es aus Kostengründen. Umgekehrt zeigt die Scientific Community eine nicht wirklich durchschlagende Initiative, dass Ideen und Demonstratoren ihren Weg in praktische Anwendungen finden.

Auf Grund der vergleichsweise kurzen Lebenszyklen der IT-Endgeräte besitzen bis 2013 80% aller stationären (PCs) sowie 100% der mobilen Endgeräte (Notebooks, PDAs, Handys) einen TPM-Chip. Ab 2009 wird für alle Notebooks von den Herstellern serienmäßig eine Software mitgeliefert, mit deren Hilfe das TPM aktiviert werden kann. Vorreiter wie z. B. der Hersteller HP oder DELL haben diesen Schritt bereits 2006/2007 vollzogen. HP bietet mit Hilfe seiner HP-Trusttools alle Notebookbesitzern die Möglichkeit, durch Verschlüsselung der Festplatte ihre Daten prophylaktisch für den Fall eines Diebstahls des Endgerätes gegen Ausspähung zu schützen. Allerdings existieren im Markt entsprechende Softwareprodukte, die auch ohne Rückgriff auf das TPM entsprechende Funktionalitäten wie z. B. eine Festplattenverschlüsselung anbieten.

Bei der TCG schreiten die Standardisierungs-Aktivitäten langsam voran, wobei der Schwerpunkt auf dem Standard für mobile Endgeräte und Netzwerkarchitekturen liegt. Es besteht weiterhin der Eindruck, dass entsprechende Aktvitäten der Mitglieder darauf beruhen, Know-how einzubringen, dass bereits in irgendeiner Form wie z. B. durch Patente geschützt ist. Auch werden Vermutungen darüber, dass marktmächtige Akteure im Bereich Hardware und Software, die bei der TCG mitarbeiten, parallel an proprietären Lösungen arbeiten, nicht entkräftet.

Wesentliche TC-Aktivitäten im industriellen Bereich konzentrieren sich weiterhin im Bereich des Automobil- und LKW-Baus. Bis 2013 werden eine Reihe von Automobil- und LKW-Serien vorgestellt, deren Tachometer bzw. Fahrtenschreiber als vollkommen manipulationssicher gelten. Von der breiten Öffentlichkeit werden diese Aktivitäten jedoch nur beiläufig wahrgenommen. Die entsprechenden Zulieferer kündigen an, bis 2013 die jeweiligen Komponenten ausschließlich mit TC-Technik fertigen zu wollen. Der manipulationssichere Tachometer wird insbesondere für den Gebrauchtwagenmarkt als von hoher Bedeutung eingeschätzt, da er Vertrauen zwischen privaten Vertragspartnern schafft und eine große Hürde gegen Betrug errichtet.

Entsprechende Entwicklungen werden auch von der Toll Collect GmbH in Betracht gezogen. Ab 2013 soll keine On-Board-Unit mehr ohne TPM-Funktionalität beschafft werden. Diese Entscheidung wurde von Toll Collect prophylaktisch getroffen, obwohl bislang keine Fälle von Missbrauch öffentlich bekannt wurden. Ähnliche Überlegungen werden bei den Herstellern von Settop-Boxen für Kabelnetze sowie IPTV-Dekoder angestellt, um Manipulationsmöglichkeiten sowie nicht-autorisierten Zugang zu durch Conditional Access geschützten Programmen grundlegend zu verhindern. Besonderer Wert wird hierbei auf das Zusammenspiel von Smart Card und TPM gelegt.

Auf Grund einzelner Beispiele in den USA beginnen auch in Deutschland sich einzelne Akteure für den Einsatz von TC-Technologie im medizinischen Bereich zu interessieren. Wichtige Dokumente im Diagnose- sowie im Abrechnungsbereich erhalten zum Zeitpunkt ihrer Entstehung einen digitalen Zeitstempel und eine ID, die Transparenz und Nachprüfbarkeit schaffen und den jeweiligen Erzeuger bzw. Bearbeiter ausweisen. Bis 2013 werden einige Anwendungspilote ins Leben gerufen, die jedoch auf Grund der bescheidenen Ausstattung mit Mitteln keine kurzfristig vermarktbaren Resulte vorweisen können. Im Bereich des Enterprise Rights Management zeigen sich erste Beispiele für die Gestaltung des Zugriffs und der Verwendung von Unternehmensdaten. Dies gilt etwa auch für die Ablage von Konstruktionsplänen etwa in der Luftfahrtindustrie.

Als ein weiteres interessantes Anwendungsfeld erweist sich der Bereich der Call Center. Mit der sukzessiven Umstellung auf VoIP ist es möglich geworden, den Datenfluss eines VoIP-Telefonats kontinuierlich mit einem Zeitstempel und einem Nachweis der Unverfälschtheit zu versehen. Vor diesem Hintergrund ergibt sich die Möglichkeit, Kundengespräche über Produkte, Vertragsabschlüsse, Vertragsumgestaltung sowie Vertragskündigungen weitgehend papierlos abzuwickeln. Erste Pilotprojekte signalisieren eine vorsichtige Akzeptanz der Verbraucher, während die Kundenbetreuungscenter hierdurch erhebliche Effizienzgewinne realisieren können. In der telefonischen Direktvermarktung werden neue Geschäftsmodelle ermöglicht, die jedoch auf Vorbehalte des Verbraucherschutzes stoßen.

Mit der langsamen Verbreitung von Smart Metern, die zur Steigerung der Energieverbrauchseffizienz vor allem in Unternehmen, nach und nach aber auch in privaten Haushalten bis 2013 Verbreitung finden, findet sich ein weiterer Anwendungsbereich,

der den Einsatz der TC-Technologie in bestimmten Produkten vorsieht, deren Einsatz auf ihrer Vertrauenswürdigkeit basiert. Nach Einschätzung der Hersteller eignet sich die TC-Technologie, um Smart Meter definitiv gegen Manipulationsversuche von außen zu schützen. Entsprechende Vorkommnisse zeigen, dass selbst fachkundige und gewiefte Manipulationsversuche an der neuen Technik scheitern, da diese schnell entdeckt werden.

Auf Grund der positiven Erfahrungen in diesem Bereich migriert die TC-Technologie allmählich auch in andere Bereiche der Übertragungs- und Messtechnik, vor allem im Umweltbereich. Auf Grund der verhaltenen Entwicklung werden Forderungen laut, der Gesetzgeber solle definierte Sicherheitsstufen entsprechend den Common Criteria in bestimmten Anwendungsfeldern festschreiben und dadurch der Marktentwicklung einen Schub verleihen.

Angesichts des verhaltenen Interesses der industriellen Akteure werden von Seiten der Scientific Community vermehrt Anstrengungen unternommen, um weitere Mittel für Grundlagen-bezogene sowie anwendungsrelevante F&E-Aktivitäten einzuwerben. Trotz einiger Erfolge wird mit diesen Projekten das grundsätzliche Dilemma der Scientific Community nicht sehr wesentlich relativiert. Zum einen binden die Einwerbungsaktivitäten von Drittmitteln einen nicht unwesentlichen Teil der Ressourcen, die für eine intensivere Befassung mit den noch offenen Problemstellungen und Fragen der Grundlagenforschung erforderlich wären. Zum anderen reichen diese Mittel nicht aus, um den Durchbruch hin zu marktrelevanten industriellen Massenmarktanwendungen zu beschleunigen. Vereinzelt werden kritische Stimmen laut, die darauf hin weisen, dass Deutschland auf Grund seiner zögerlichen Haltung bei TC Gefahr läuft, seine Meinungs- und Marktführerschaft an Länder wie China, die USA und Japan zu verlieren.

Auch die öffentlichen Hände sind angesichts der bestehenden Unsicherheiten über die faktische Marktrelevanz der TC-Entwicklung eher zögerlich, weitere F&E-Mittel in größerem Umfang zur Verfügung zu stellen. Dies gilt auch für die Ebene der EU, die die Fortführung der bestehenden Forschungsaktivitäten wie z. B. ROBIN unter den Vorbehalt eines Nachweises der Anwendungsrelevanz gestellt hat.

Politische Handlungsoptionen

Das Trendszenario beinhaltet für die Formulierung politischer Handlungsoptionen die größten Unsicherheiten, da die meisten aus heutiger Sicht erkennbaren Lösungen und Anwendungen offenkundig dem Markt voraus laufen, so dass eine echter Mehrwert aus heutiger Sicht plausibel vermutet, aber nicht eben wirklich dokumentiert werden kann. Diese Situation entspricht jedoch den bei vielen Innovationen abzuarbeitenden typischen Investitionsrisiken: Entscheidungen können in einer Situation wie dieser nur unter Inkaufnahme von Unsicherheiten und zu begrenzenden Risiken getroffen werden.

Es geht daher im Kern dieses Szenarios darum, mögliche Entwicklungspfade durch einen begrenzten und gezielten sowie möglichst effizienten Einsatz von Ressourcen offenzuhalten. Ferner sind alle relevanten nationalen und internationalen Entwicklungen durch den Einsatz entsprechender Instrumente einem *kontinuierlichen Monitoringprozess* zu unterwerfen. Der TC-relevante Diskurs und Informationsfluss zwischen den nationalen Akteuren sollte verbessert und insgesamt die Awareness erhöht werden. Ferner sollte das Know-how, dass für die Beherrschung der TC-Technologie erforderlich ist, systematisch verbessert werden. Dahinter steht die Erwartung, dass die Industrie im Zeitablauf entsprechende Anwendungsbedarfe artikulieren und ihre Umsetzung weitgehend in die eigenen Hände nehmen wird.

Angesichts der abzuwägenden Risiken in dieser durch Unwägbarkeiten geprägten Situation, nämlich: a) zu verhindern, dass zu viele öffentliche und private Mittel und Ressourcen ungerechtfertigt gebunden bzw. ineffizient verausgabt werden, sowie b), dass bestehende Know-how-Vorsprünge der deutschen Scientific Community gesichert und potenzielle industriepolitische Chancen nicht vergeben werden sollen, - legen wir nahe, im Rahmen des Trendszenarios folgende Optionen in Betracht zu ziehen:

1. Weitere Mitarbeit und Beeinflussung der Arbeit der TCG durch deutsche Akteure, um den kontinuierlichen Know-how-Transfer zu gewährleisten und um Einblick in die weiteren Standardisierungsaktivitäten zu behalten. Einladung der deutschen TCG-Mitglieder z. B. zur (jährlichen) Berichterstattung bei den Branchenverbänden TeleTrusT, ggf. BITKOM. Präsentationen zum jeweiligen Status Quo auf einschlägigen Industriemessen wie z. B. der CeBIT zur Verbesserung der Awarness gegenüber TC.

2. Gezielte Gespräche mit Vertretern von Unternehmen bzw. Durchführung von Fokusgruppen, bei denen eine hohe IT-Sicherheit Teil des Geschäftsmodells ist wie z. B. Banken, Versicherungen, Krankenhäuser und bei denen der Zugriff auf prozessrelevante Daten besonders sensibel ist wie z. B. bei Technologieträgern (Ingenieur- und Konstruktionsbüros).

3. Einflussnahme auf die EU, im Rahmen eines langfristig angelegten Forschungsprogramms weitere Mittel für eine gebündelte und fokussierte TC-Forschung in Europa zur Verfügung zu stellen (in Ergänzung oder bzw. auch als Verlängerung von ROBIN) und darauf hinwirken, dass hieran deutsche Akteure weiter an prominenter Stelle mitwirken.

4. Mobilisierung von Mitteln zur Einrichtung einer Stiftungsprofessur, um die Know-how-Trägerschaft Deutschlands auszubauen.

5. Systematisches Monitoring der nationalen sowie insbesondere der internationalen TC-Entwicklung (unter deutlicher Ausweitung der Vergleichsmärkte auf alle besonders aktiven TC-Nationen) im Rahmen eines jährlich oder zweijährlich zu erstellen-

den Gutachtens, um rechtzeitig über wichtige Entwicklungen Informationen zu beschaffen. Präsentation und Diskussion der Ergebnisse in den Branchenverbänden.

6. Systematisches Monitoring zur Evaluierung der allgemeinen mittel- und langfristigen Entwicklung der IT-Hard- und Software-Märkte mit Fokus auf deren industrie- sowie sicherheitsrelevanten Aspekte sowie der Entwicklungsstrategien der wichtigsten internationalen Spieler unter Berücksichtigung von TC.

7. Definition von prioritär zu behandelnden Kernaspekten der TC-Technologie sowie Festlegung von Schwerpunkten in Zusammenarbeit mit der Scientific Community, die im Rahmen begrenzter Förderprojekte oder auch als PPP konzertiert bearbeitet werden sollten. Prüfung der Weiterentwicklung und Optimierung der Mikrokernelentwicklung, Virtualisierungsstrategien, Konformitätsprüfungen: Entwicklung einer nationalen F&E-Agenda (Roadmap) sowie Festlegung entsprechender prioritärer Entwicklungsziele unter Einbeziehung der relevanten Akteure. Da diese Akteure sich in einer deutlichen Wettbewerbssituation befinden, sollte ein neuer Modus der Kooperation gefunden werden z. B. durch die Institutionalisierung eines Beirates. Besonders wichtig wäre eine systematische Begleitung dieser Aktivitäten z. B. durch die Experten des Bundesamtes für Sicherheit in der Informationstechnologie (BSI).[343]

8. Erarbeitung einer TC-Broschüre oder vergleichbarer Materialien oder Multimedien zum State-of-the-Art als Basis für die Schaffung einer sektorübergreifenden Awareness.

9. Organisation eines nationalen TC-Gipfels: Die TC-Scientific Community sowie die ITK-Branche treffen im Rahmen moderierter Workshops auf Vertreter der potenziellen Anwenderindustrien. Diesem Schritt kommt besondere Bedeutung zu, da ein Dialog zwischen den Akteuren bisher nur unzureichend stattfindet. Dieser Dialog kann einen wichtigen Beitrag zur Klärung der Frage leisten, wie relevant TC für die übrige Industrie ist, wo primär wichtige Anwendungsfelder liegen (z. B. Embedded Systems) und welche wirtschaftlichen Potenziale hierdurch erschlossen werden können. Da Fraunhofer SIT über langjährige Kooperationsbeziehungen mit Industrieunternehmen verfügt, scheint dieses Institut aus der Sicht verschiedener Experten besonders geeignet, einen solchen Dialog im Auftrag der Politik zu initiieren.

10. Prüfung einer F&E-Strategie, inwieweit durch Pilotprojekte im öffentlichen Sektor etwa im Bereich eGovernment oder durch PPP etwa bei eBanking initiale Anwendungsfelder ausgelotet und in Hinblick auf ihren Beitrag zur Lösung von IT-Sicherheitsproblemen evaluiert werden können.

---

343 Die Rolle des BSI geht jedoch hierüber weit hinaus, wie die jüngste Ausschreibung des Projektes 660e „Trusted Software Stack und darauf aufsetzende Applikationen / Dienste (TSS) zeigt. Vgl. http://www.bsi.de/ausschr/einkauf/TSS.htm.

11. Überlegungen bzgl. der Einleitung eines Kartellverfahrens: Nachdem die entsprechenden Bedenken seit Jahren bekannt sind, ohne dass die TCG den Zugang zu den relevanten (höheren) Mitgliedskategorien diskriminierungsfrei ausgestaltet hat, sollte deshalb auf die unverzügliche Einleitung eines diesbezüglichen Kartellverfahrens hingewirkt werden. Diese Feststellung besitzt auch Gültigkeit bzgl. der anderen beiden Szenarien.

9.2 Trusted Computing: Das Wachstumsszenario (bester Fall)

Angesichts der vergleichsweise kurzen Lebenszyklen der IT-Endgeräte besitzen bis 2013 100% aller stationären (PCs) sowie alle mobilen Endgeräte (Notebooks, PDAs, Handys) ein TPM. Ab 2008 wird für alle Notebooks von den Herstellern serienmäßig eine Software mitgeliefert, mit deren Hilfe das jeweilige TPM aktiviert werden kann. Ein mitgeliefertes Schulungstool unterstützt Nutzer bei der Aktivierung und Nutzung der Funktionalitäten, klärt über Sicherheitsaspekte sowie Einsatzmöglichkeiten auf. Seit die Nutzung dieser Funktionalität voranschreitet, geht der Diebstahl von Notebooks signifikant zurück.

Im Internet werden auf den entsprechenden Portalen auf der Basis von Open Source zahlreiche Tools zur Verfügung gestellt, mit deren Hilfe die Funktionalitäten der TPMs auf Desktop-Geräten aktiviert bzw. ihr Status überprüft werden kann. Auf Grund der stark wachsenden Verbreitung von Mobile Enterprise Solutions in Unternehmen sowie der zunehmenden Anwendung von mobilem eGovernment und eBanking weisen die Vertriebsabteilungen der Hersteller auf die steigenden Sicherheitsanforderungen hin und werben aktiv für den Einsatz von TC-Funktionalitäten insbesondere für die Datenverschlüsselung. Nach und nach werden von den Nutzern mobiler Endgeräte alle wesentlichen Funktionalitäten angewendet, wie sie auch über fixe Internetzugänge genutzt werden. Dies steigert das subjektive Sicherheitsbedürfnis der meisten Nutzer und ebnet den Weg für die aktive Nutzung von TC in mobilen Geräten.

Im Bereich der Desktop Rechner bieten immer mehr Hersteller die Möglichkeit, durch den Einsatz einer Smard Card den Zugang zu ihrem jeweiligen PC zu autorisieren. Auf diese Weise werden die Sicherheit einer personalisierten Smart Card mit den Funktionalitäten des TPM verknüpft. Auf Grund des Erlasses einer Vorschrift wird der Einsatz beider Lösungen bei allen Behördenrechnern obligatorisch. Experten schlagen vor, durch die Entwicklung entsprechender Schnittstellen den Einsatz von Smart Cards durch den Elektronischen Personalausweis oder die Gesundheitskarte zu ersetzen.

Angesichts der weltweit zunehmenden Bedrohungssituation in den offenen Telekommunikationsnetzen sowie der stark zunehmenden Internetkriminalität beschlenigt die TCG ihre Standardisierungsaktivitäten und kündigt an, bis 2013 für alle Anwendungsbereiche entsprechende Standards zu verabschieden. Auf diese Weise sollen alle Herstel-

ler hinreichende Sicherheit erhalten. Die Zahl der in der TCG aktiven Unternehmen steigt deutlich an.

Immer mehr Industriebranchen in Deutschland beginnen die Potenziale von TC für ihre Produkte zu nutzen. In einer immer größeren Anzahl von Geräten, Maschinen und Produkten, in denen Rechner-basierte Funktionen zum Einsatz kommen und Bereiche, in denen vitale elektronische Prozesse und Daten geschützt werden müssen, werden TPMs implementiert. Den Herstellern von Werkzeugmaschinen z. B. gelingt es auf diese Weise, den Schutz ihres Know-hows auch beim Verkauf ihrer Produkte ins Ausland sukzessive zu verbessern. Durch die Implementierung dieser Sicherheitsfunktion wird die Attraktivität der Produkte nicht unwesentlich gesteigert. IT-Sicherheit wird zu einem weiteren wichtigen Differenzierungsmerkmal im internationalen Wettbewerb der Hersteller. Der TÜViT entwickelt ein eigenes Zertifikat mit dem Label: „TC-certified“.

Als ein wesentliches Anwendungsfeld erweist sich zunehmend des Enterprise Rights Management. Die Gestaltung und das Management von IT-Prozessen in Unternehmen wird durch den Einsatz von TC-Technologie deutlich vereinfacht.

Neben dem Automobil- und LKW-Bau sowie dem Maschinen- und Industrieanlagenbau interessieren sich zunehmend auch der Bankensektor, der Versorgungssektor (Strom, Wasser, Gas), die Telekommunikationsindustrie sowie der medizinische Sektor für den Einsatz von TC-Technologien. Auf den einschlägigen Industriemessen werden zunehmend Produkte, deren Hard- und Software TC-Elemente beinhalten, vorgestellt und aktiv vermarktet.

Offenkundig eignen sich alle Anwendungsbereiche, in denen die zum Einsatz kommende Hard- und Software nach ihrer Implementierung nicht ständigen Veränderungs- bzw. Anpassungsprozessen unterliegt, in besonderer Weise für den Einsatz von TC. Hierbei werden besondere Marktchancen in allen Bereichen der Machine-to-Machine-Kommunikation gesehen.

Auf Grund der Entwicklung bei TC-Anwendungen erwarten deutsche Unternehmen und Dienstleister einen zunehmend härteren Wettbewerb um erfolgreiche Markteinführungsstrategien durch ausländische Hersteller.

Vor diesem Hintergrund wird die Forderung erhoben, durch förderpolitische Maßnahmen den Transfer von TC-Technologien in die Industrie zu beschleunigen, um verlorenes Terrain zurückzugewinnen. Der Verlust der Marktführerschaft soll durch einen nationalen Ideenwettbewerb, bei dem die attraktivsten Projektideen der sich bewerbenden Konsortien ausgezeichnet und anschließend zu 50% öffentlich gefördert werden, zurück gewonnen werden.

Fast alle Rechner, mobile Endgeräte sowie elektronische Rechenkomponenten werden inzwischen im asiatischen Ausland gefertigt und von dort importiert. Die meisten dieser

Produkte und Komponenten sind mit einem TPM ausgerüstet. Vor diesem Hintergrund wird aus wirtschaftichen und politischen Gründen von den Wirtschaftsverbänden die Notwendigkeit betont, zum einen beim Einkauf auf die Verwendung bestimmter TC-Komponenten zu achten. Zum anderen wird gefordert, dass deren Konformität mit den geltenden TCG-Standards zu überwachen sei. Es wird angeregt, diese Konformität zu prüfen, in dem Geräte oder Komponenten einem standardisierten Prüfverfahren unterworfen werden. Dieses Prüfverfahren soll durch den vom BSI zertifizierten TÜViT standardisiert und mittels Test Beds angewendet werden. Es wird von Seiten der Industrieverbände darauf gedrungen, einen gemeinsamen europäischen Standard zur Sicherstellung der Verwendung bestimmter Hardware-Komponenten durch die Produzenten in Kraft zu setzen. Es stehen Überlegungen im Raum, eigene Produktionskapazitäten für IT-Hardware in Europa aufzubauen.

Angesichts der gestiegenen industriepolitischen Bedeutung von TC steigen offenkundig die Anreize für manche Hardware-Hersteller, die Transparenz bzgl. der Funktionalitäten von TPMs zurückzunehmen bzw. diese zu verschleiern. So wird auf einschlägigen Foren im Internet heftig darüber debattiert, welche Folgen mit der Migration von TPMs in die CPU verbunden sein könnten. Auf Grund von Skalenerträgen gilt es inzwischen als sicher, dass TPMs künftig mit die CPUs bzw. Chipsätze integriert werden. In diesem Zusammenhang wird auf die Möglichkeiten von Hidden-Channels verwiesen und die öffentlichen Stellen werden aufgefordert, gegen derartige Hardware vorzugehen und entsprechende Verifikationstools einzusetzen.

Angesichts der Tatsache, dass auch die öffentlichen Institutionen aus Kostengründen auf COTS zurückgreifen, sollen bei allen Geräten für den Einsatz in Sicherheitsklassifizierten Bereichen entsprechende Tests vorgeschrieben werden.

Politische Handlungsoptionen

Das Wachstumsszenario beinhaltet in Hinblick auf politische Handlungsoptionen mittlere Unsicherheiten, da die industriellen Akteure mehr oder minder zeitnah und klar einen Bedarf artikulieren sowie verschiedene Anwendungsszenarien in ihr innovationspolitisches Denken und Handeln integrieren. Zwar ist ein faktischer Mehrwert nur in Ansätzen realisiert, allerdings bestehen hohe Erwartungen, dass TC-Technologie als Enablertechnologie einen Beitrag zur Steigerung der internationalen Wettbewerbsfähigkeit leisten kann. Allerdings haben inzwischen andere, z. T. auch marktdominante Akteure Entscheidungen getroffen, TC im Rahmen einer innovationspolitischen Strategie systematisch in ihre Produkte zu integrieren. In diesem Zusammenhang werden auch zunehmend Fragen des Wettbewerbs- und Kartellrechts relevant.

Vor diesem Hintergrund geht es im Kern des Wachtumsszenarios darum, alle innovationsrelevanten Kräfte zu bündel und zu koordinieren, bestehende Impulse aufzugreifen und zu unterstützen sowie einen Dialog zu institutionalisieren, um kurzfristig eine branchenübergreifende Implementierungsstrategie anzustoßen. Alle Anwendungspotenziale

sollen schnell und breitenwirksam mobilisiert werden. Ein gezielter Einsatz von öffentlichen und privaten Ressourcen und Mitteln soll dafür sorgen, dass Anschluss gehalten werden kann an diejenigen Länder, die inzwischen zu Deutschland aufgeschlossen bzw. es überholt haben.

In dieser Situation geht es zum einen darum, in welcher Weise die Eigeninitiative der Industrie stimuliert sowie private Mittel und Ressourcen mobilisiert werden können. Zum zweiten geht es um die Frage, ob und in welcher Weise der Einsatz öffentlicher Mittel und Ressourcen dazu beitragen kann, diesen Prozess zu unterstützen, um das bestehende Know-how der deutschen Scientific Community zu sichern und dieses Wissen möglichst schnell und breitenwirksam in industriepolitische Chancen und Anwendungen umzumünzen. Im Rahmen des Wachtumsszenarios sollten daher – zusätzlich zu den Maßnahmen des Trendszenarios - folgende Optionen überdacht werden:

1. Ausbau und Intensivierung der Mitarbeit und Beeinflussung der Arbeit der TCG durch deutsche Akteure, um den Know-how-Transfer zu gewährleisten. Einladung der deutschen TCG-Mitglieder z. B. zur kontinuierlichen Berichterstattung bei den Branchenverbänden Teletrust sowie BITKOM. Präsentationen zum jeweiligen Status Quo auf einschlägigen Industriemessen wie z. B. der CeBIT zur Verbesserung der Awarness gegenüber TC.

2. Systematisches Monitoring der internationalen TC-Entwicklung (unter Betrachtung der innovationskräftigsten Vergleichsmärkte) mit dem Ziel, die wichtigsten Entwicklungen möglichst zeitnah zu erfassen und deren Relevanz für deutsche Unternehmen und Behörden in Hinblick auf ihre Übertragbarkeit zu analysieren. Systematische Verbreitung der Ergebnisse durch die Bundesregierung, BSI und Verbände hin zu den potenziellen Anwendern im Rahmen einer Ausweitung der Lissabon-Strategie.

3. Festlegung der wichtigsten F&E-Schwerpunkte im Rahmen eines nationalen Förderprogramms zur Beschleunigung der Umsetzung in Produkte und Anwendungen. Zielgerichtete Förderung wichtiger Grundlagenaspekte durch öffentliche Mittel in vorwettbewerblichen Anwendungsbereichen. Unterstützung der Zusammenarbeit zwischen der Scientific Community und der Industrie durch Bereitsstellung von Mitteln für einen über mehrere Jahre laufenden Förderwettbewerb von Initialprojekten. Nach einer Ausschreibung werden die wichtigsten Projektideen der Konsortien aus Forschung und Industrie prämiert und teilgefördert. Im Rahmen einer Begleitforschung werden im Rahmen einer Technik- sowie Rechtsfolgenabschätzung die gesellschaftlichen Implikationen der Einführung von TC begleitend untersucht. Die Sicherung der gesellschaftlichen Akzeptanz von TC ist ein wichtiger und akzeptanzfördernder Baustein in der Kette der Vertrauensgenerierung.

4. Der Branchenverband TeleTrusT stellt mit Hilfe seines TC-Arbeitskreises eine Plattform zur Verfügung, über die ein breiter branchenübergreifender Dialog organisiert wird. Durch Erstellung von Informationsmaterialien und Multimedia zum State-of-the-Art und deren Verbreitung z. B. auf Industriemessen werden die Grundlagen für die Generierung von industrieweiter Awareness geschaffen. Im Rahmen des TC-Arbeitskreises werden Vertreter der Verbraucherverbände, des Datenschutzes, des TÜViT, des BSI etc. sowie der deutschen TCG-Mitglieder eingebunden, um frühzeitig Probleme der Akzeptanz, des Datenschutzes sowie der Nutzerfreundlichkeit behandeln zu können. Hierfür wird ein eigenes Internet-Portal für den Dialog mit der Internet Community gestartet.

5. Entwicklung und Abstimmung einer TC-Strategie auf Ebene der EU. Vorbereitung und Verabschiedung einer entsprechenden TC-Mitteilung durch den EU-Ministerrat.

6. Entwicklung und Implementierung von haftungsrechtlichen Regelungen, die im Wesentlichen in Analogie zum Haftungsrecht der digitalen Signatur entwickelt werden können.

9.3 Trusted Computing: Das Stillstands-Szenario (schlechtester Fall)

Das Stillstand-Szenario beinhaltet für die Formulierung politischer Handlungsoptionen die geringsten Unsicherheiten, da hierbei die meisten - aus heutiger Sicht erkennbaren Lösungen und Anwendungen - offenkundig an den Anforderungen der Märkte vorbei laufen, so dass aus heutiger Perspektive eine echter Mehrnutzen - nicht zuletzt auch im Verhältnis zum Aufwand - auch langfristig nicht leicht erkennbar ist. Das Stillstand-Szenario ist das Szenario, mit dem sich im Wesentlichen nur Aktivitäten im Bereich der Grundlagenforschung legitimieren lassen, um potenzielle Entwicklungspfade nicht gänzlich zu verschütten und um den Know-how-Vorsprung Deutschlands zu sichern.

Es geht daher im Kern dieses Szenarios darum, mögliche Entwicklungspfade, die aus heutiger Sicht sinnvoll und plausibel erscheinen, durch einen sehr begrenzten und hocheffizienten Einsatz begrenzter Ressourcen offenzuhalten und zu begleiten bis zu einem im weiteren Prozess zu definierenden Punkt, an dem eine weitere oder sogar abschließende Entscheidung über TC und seine industriepolitische Betrachtung getroffen werden kann.

Ein solcher begleitender Prozess kann sich u. U. noch einige Jahre hinziehen und über das Jahr 2013 hinausreichen. Der Einsatz von öffentlichen F&E-Ressourcen sollte in diesem Szenario minimiert werden und alle relevanten nationalen und internationalen Entwicklungen eher durch den Einsatz von begrenzten Monitoringaktivitäten geprägt sein. Bis dahin sollte der TC-relevante Diskurs und Informationsfluss zwischen den na-

tionalen Akteuren mit dem Ziel verbessert werden, zu einer gemeinsamen und am aktuellen Prozess orientierten, möglichst validen Einschätzung bzgl. der künftigen Perspektiven von TC zu gelangen.

Wegen der eher kurzen Lebenszyklen der IT-Endgeräte besitzen bis 2013 80% aller stationären (PCs) sowie 100% der mobilen Endgeräte (Notebooks, PDAs, Handys) einen TPM-Chip. Obwohl manche Hersteller eine entsprechende Software mitliefern, werden nach aktuellen Marktumfrage die Funktionalitäten des TPM nur von sehr wenigen Notebook-Besitzern tatsächlich genutzt. Außerdem werden von IT-Herstellern Softwareprodukte vermarktet, die auch ohne Rückgriff auf das TPM entsprechende Sicherheits-Funktionalitäten anbieten. Allerdings werden auch diese Tools wegen unzureichender Nutzerfreundlichkeit nur sehr begrenzt genutzt. Immer mehr Unternehmen gehen deshalb dazu über, im Rahmen ihrer IT-Sicherheits-Policy ihre Außendienstmitarbeiter zur Nutzung und Aktivierung der Sicherheitsfeatures zu verpflichten.

Bei der TCG schreiten die Standardisierungs-Aktivitäten in den einzelnen Arbeitsgruppen nur zögerlich voran. Marktumfragen wichtiger TCG-Akteure signalisieren eine nur geringe Akzeptanz für TC-Lösungen. Die Zahl der in der TCG aktiven Unternehmen sinkt daher seit Jahren kontinuierlich.

Unterdessen steigen alle Formen devianten Verhaltens, der Mißbrauch und die Internetkriminalität kontinuierlich an. Immer mehr Staaten drängen daher darauf, dass die Cybercrime Convention von allen Staaten unterzeichnet wird. Außerdem wird immer nachdrücklicher die Gründung einer eigenen internationalen Verfolgungsbehörde für Internetstraftaten gefordert, der grenzüberschreitende Kompetenzen eingeräumt werden sollen. Gleichzeitig signalisieren repräsentative Umfragen, dass die Bevölkerung, aber auch die Mehrzahl der Unternehmen, sich mit den Zuständen im Internet abfindet und etwa bestimmte Nutzungseinschränkungen wie z. B. durch Spamming und auch andere Formen des Mißbrauchs nolens volens akzeptiert.

Aktivitäten zur Umsetzung von TC-Anwendungen im industriellen Bereich sind bis auf wenige Ausnahmen zum Erliegen gekommen und konzentrieren sich im wesentlichen auf den Bereich des Automobil- und LKW-Baus. Bis 2013 werden eine Reihe von Automobil- und LKW-Serien vorgestellt, deren Tachometer bzw. Fahrtenschreiber als manipulationssicher gelten, allerdings ist die Branche noch ein Stück davon entfernt, diese Anwendungen zum Standard zu machen bzw. in der Serie zu verbauen. Von der breiten Öffentlichkeit werden diese Aktivitäten kaum wahrgenommen, so dass sich hierdurch auch bei der Vermarktung der Produkte keine Vorteile generieren lassen.

Auch im Ausland sind, mit Ausnahme einiger Staaten mit autoritären Regimes, die Aktivitäten zur Umsetzung und Verbreitung von Trusted Computing zurückgefahren worden. Für fast alle wichtigen Funktionalitäten von TC existieren Substitute und der Markt ist bereit, die damit verbundenen potenziell höheren Sicherheitsrisiken zu akzeptieren.

Die bis 2013 ins Leben gerufenen Pilote werden nur noch eingeschränkt fortgeführt oder eingestellt, da keine wirklich überzeugenden Perspektiven bzgl. des Zusatznutzens erkennbar werden, die den Transfer von TC-Lösungen in den Massenmarkt verbessern könnten. Die vergleichsweise geringen Mittelausstattungen für F&E-Aktivitäten tragen dazu bei, dass allenfalls sehr langfristig sicherheits- sowie wirtschaftlich attraktive Anwendungspotenziale erwartet werden.

Angesichts des geringen Interesses der industriellen Akteure werden von Seiten der Scientific Community nur vereinzelt Erfolge vermeldet, dass Mittel für grundlagenbezogene sowie anwendungsrelevante F&E-Aktivitäten eingeworben werden konnten. Einschlägige Aktvitäten konzentrieren sich im Wesentlichen auf Fragen der Grundlagenforschung.

In Bezug auf eine TC-Förderung durch die öffentlichen Hände gibt es in Hinblick auf die ungewissen Perspektiven nur geringe Anreize, F&E-Mittel zur Verfügung zu stellen. Dies gilt auch für die Ebene der EU, die die Fortführung der bestehenden Förderaktivitäten eng an die Kooperation mit Industriekonsortien gebunden hat. Vor diesem Hintergrund sollten die nachfolgend skizzierten Handlungsoptionen geprüft werden.

1. Weitere Mitarbeit und Beeinflussung der Arbeit der TCG durch deutsche Akteure, um den Know-how-Transfer zu gewährleisten. Einladung der deutschen TCG-Mitglieder z. B. zur gelegentlichen Berichterstattung beim Branchenverband TeleTrusT.

2. Einflussnahme auf die EU, im Rahmen eines langfristig angelegten Forschungsprogramms (8. Rahmenprogramm) bestimmte Mittel für eine gebündelte TC-Forschung zur Verfügung zu stellen (in Ergänzung oder bzw. auch als Verlängerung von ROBIN/EMSCB) und darauf hinwirken, dass hieran deutsche Akteure weiter mitwirken.

3. Monitoring der nationalen sowie insbesondere der internationalen TC-Entwicklung (unter Ausweitung der Vergleichsmärkte auf alle besonders aktiven TC-Nationen) im Rahmen von Gutachten, die in unbestimmten Zeitintervallen vergeben werden.

4. Definition von prioritär zu behandelnden Kernaspekten der TC-Technologie sowie Festlegung von Schwerpunkten in Zusammenarbeit mit der Scientific Community, die im Rahmen begrenzter Förderprojekte oder auch als PPP konzertiert bearbeitet werden sollten. Weiterentwicklung bzw. Optimierung der Mikrokernelentwicklung sowie von Virtualisierungsstrategien.

5. Sporadische Befassung mit TC bei den Industrieverbänden mit Unterstützung von Teletrust.

6. Erarbeitung einer TC-Broschüre oder vergleichbarer Materialien zum State-of-the-Art als Basis für die Schaffung einer sektorübergreifenden Awareness.

10 Fazit der Untersuchung

Es gibt kaum Zweifel, dass sich die Bedrohungslage im World Wide Web und die allgemeine Risikosituation in den nächsten Jahren kontinuierlich zuspitzen werden. Daher wächst der Bedarf an technischen und organisatorischen Lösungen, um die Vertrauenswürdigkeit und Verlässlichkeit der Informations- und Telekommunikationsinfrastruktur und der darauf basierenden Anwendungen auf ein möglichst hohes Niveau zu heben und zu sichern. Trusted Computing bietet nach Einschätzung der meisten im Rahmen dieser Studie befragten Akteure einen Weg und ein erhebliches Potenzial, für diese Herausforderungen und Ansprüche Lösungsbeiträge zu liefern.

In Hinblick auf die Implementierung dieser Technologie in Embedded Systems wird TC sogar der Charakter einer Schlüsseltechnologie zugesprochen. Aber auch etwa im Kontext von Enterprise Rights Management, dem Management von IT-Prozessen in Unternehmen, digitalen Zeitstempeln oder der elektronischen Dokumentenverwaltung werden wichtige Anwendungsfelder gesehen.

Mit dieser industriellen Nutzenperspektive ist die *positive Seite* der „Janusköpfigkeit“ von TC umschrieben. Um die vermuteten oder erwarteten Potenziale von TC tatsächlich zur Entfaltung zu bringen, sind vielfältige Schritte erforderlich. Diese Schritte erfolgen unter einem hohen Maß unvollständiger Informationen. Sie bergen somit Risiken z. B. in Hinblick auf die Fehlallokation von F&E-Mitteln. IT-Sicherheit bzw. TC erscheint jedoch zu wichtig, als dass es sich nicht lohnen würde, die bestehenden Unwägbarkeiten und offenen Fragen zu verringern und das Nutzenpotenzialversprechen dieser Technologie einer genauen Prüfung zu unterziehen.

Zunächst ist festzuhalten und auch unstrittig, dass Deutschland im internationalen Vergleich – nicht zuletzt durch die vorausschauende Politik des BMWI - eine herausragende Position bei TC einnimmt. Mit EMSCB wurden wichtige Grundlagen und Voraussetzungen im Bereich der Miniaturisierung von Betriebssystemen (Mikrokernel-Architektur) geschaffen. Ihre Weiterentwicklung sollte daher ein wichtiger Baustein einer in Zusammenarbeit mit den relevanten Akteuren zu definierenden deutschen TC-Roadmap sein. Ein weiterer wichtiger Baustein dieser Roadmap sollte der Technologietransfer dieser Grundlagen (Demonstratoren, Konzepte) hin zur industriellen Anwendungsreife bilden. Dieser Schritt wird in der derzeitigen Situation als besonders wichtig angesehen und sollte am besten im Rahmen industrieller Initialprojekte geschehen.

Die Durchführung von Initialprojekten unter breiter Beteiligung der Industrie erscheint als einzig gangbarer Weg, den erforderlichen Technologietransfer zu bewerkstelligen. Im schlechtesten Falle würde sich durch diese Aktivitäten erweisen, dass der Nutzen von TC überschätzt wurde und dieser sich eher auf Nischenanwendungen beschränkt. Auf der Haben-Seite bliebe allerdings das verbreiterte und vertiefte Know-How sowie die Gewißheit, dass nichts unversucht gelassen wurde, TC für industrielle und gesell-

schaftliche Zwecke nutzbar zu machen. Im besten Falle aber würden die Potenziale von TC einen wichtigen Beitrag zur Sicherung des Standortes und der Wettbewerbsfähigkeit der deutschen Wirtschaft beitragen.

Ein dritter Schritt der Roadmap sollte darin bestehen, diese Aktivitäten auf europäischer Ebene zu begleiten und sie im Rahmen gemeinschaftlicher F&E-Aktivitäten weiter zu entwickeln, wie dies bereits im Rahmen von Open TC geschieht.

Auf der *negativen Seite* der „Janusköpfigkeit“ von TC stehen zum einen die Befürchtungen, dass die Erschließung der wirtschaftlichen und gesellschaftlichen Nutzen von TC und dessen Verbreitung in Anwendungen des Massenmarktes mit den Versuchen marktmächtiger Akteure einhergeht, den Wettbewerb einzuschränken, Lock-in-Effekte zu erzeugen und u. U. die Nutzungshoheit von heute weit verbreiteten Anwendungen durch eigennützige Geschäftskalküle zu beschränken. Allerdings steht auch diese – vorab nicht von der Hand zu weisende Entwicklungsmöglichkeit - unter dem Vorzeichen unvollständiger Informationen. Im Rahmen von Szenarien und Rechtsgutachten könnte daher prophylaktisch geprüft werden, ob und in wieweit die zur Verfügung stehenden Instrumente des Wettbewerbs- und Kartellrechts sowie des Daten- und Verbraucherschutzes ausreichen, um einem Missbrauch entgegen zu wirken. Hierzu finden sich im vorliegenden Gutachten bereits fundierte Einschätzungen.

Eine *zweite negative Facette* der TC-Entwicklung könnte in mittelfristiger Perspektive darin bestehen, dass durch die weltweit zunehmende Konzentration der ITK-Hardware-Produktion in einzelnen Staaten Asiens die Möglichkeit entsteht, Funktionalitäten zu verbauen, die geeignet sind, das erforderliche Vertrauen in die Integrität einer Plattform nachhaltig zu untergraben. Dies gilt insbesondere dann, wenn für sicherheitsrelevante Anwendungen etwa im öffentlichen Sektor auf COTS-Produkte zurückgegriffen wird. Allerdings stellt dies keine TC-spezifische Problematik dar, sondern trifft auf alle im Ausland gefertigten IT-Komponenten zu.[344] Die im Rahmen der Studie befragten Experten bezweifeln zwar, dass ein solches Szenario ohne schwerwiegenden Imageverlust für die ausländischen Hersteller denkbar ist und die entsprechenden handelsrechtlichen Konsequenzen erheblich sind, jedoch ist ein derartiges Ereignis auch nicht ohne weiteres auszuschliessen. Vor diesem Hintergrund sollte einer solchen Möglichkeit *in jedem Fall* durch die frühzeitige Entwicklung geeigneter technischer Tests (Test Beds) bzw. im Vorfeld durch Evaluationen nach den CC begegnet werden. Es liegt auf der Hand, dass es für ein solches Test Bed einen internationalen Markt gibt. Die Einführung eines entsprechenden Hardware-Zertifikats, welches die Unbedenklichkeit der Nutzung von im Ausland hergestellter Harware bescheinigt, stellt eine der Maßnahmen dar, die diese Strategie begleiten könnten bzw. sollten.

---

344 Der aus heutiger Sicht einzig begehbare Weg, Vertrauen in COTS-Produkte zu schaffen, besteht in ihrer Evaluierung nach den Common Criteria.

Für beide Seiten, die positiven wie die negativen Aspekte des „TC-Gesichts“ gilt es, im Entwicklungsverlauf der nächsten Jahre einen Monitoringprozess zu implementieren, der die relevanten Akteure in Deutschland so zeitnah wie möglich über die nationalen sowie internationalen Entwicklungen in Kenntnis setzt, frühzeitig schwache und starke Signale aufnimmt und in entsprechende Handlungsempfehlungen umsetzt. Eine abwartende „laissez faire“-Haltung scheint sich auf Grund der vitalen Bedeutung von IT-Sicherheit und der „Janusköpfigkeit“ von TC von selbst zu verbieten.

Die typischen Netzwerkeigenschaften von TC machen es außerdem erforderlich, dass die wichtigen Akteure des ITK-Sektors zusammenwirken. Dies erfordert die Bildung eines entsprechenden Netzwerks bzw. die Gründung einer Kommunikationsplattform, mit deren Hilfe der Dialog zwischen der Scientific Community, den öffentlichen Institutionen (BMWi, BMI, BMBF, BSI), den Standardisierungsgremien (TCG, ISO), der Industrie sowie den Verbänden organisiert und moderiert werden kann. Der Branchenverband TeleTrusT hat die Bereitschaft signalisiert, hierbei mitzuwirken. Hier wäre auch die Plattform, um eine TC-Roadmap zu entwickeln, um die im Monitoring-Prozess gewonnen Daten zu bewerten und um die Umsetzung der im Trendszenario vorgeschlagenen Maßnahmen zu begleiten.

Literaturverzeichnis

<Kes> online (2003): Vertrauenskrise. Einsichten und Aussagen vom Trusted-Computing-Symposium, in: http://kes.info/archiv/online/03-4-012.htm, Abruf am 25.05.2007

<Kes> online (2004): Entschiedene Politik für deutsche Kryptographie, in: http://www.kes.info/archiv/online/04-2-006.htm, Abruf am 20.03.2007

Alkassar, A., Linnemann, M. (2007): Die Sicherheitsplattform TURAYA. Trusted Computing hat eine vertrauenswürdige Plattform. CeBIT 2007 in Hannover, in: http://www.internet-sicherheit.de/fileadmin/npo/artikel_berichte/TURAYA-Roadshow.pdf, Abruf am 02.05.2007

Alkassar, A., Stüble, C. (2003): Security Framework for Integrated Networks, Milcom 2003 Military Communications Conference, Saarland University, 2003

Alkassar, A., Stüble, C., Sadeghi A. (2003): Secure Object Identification – or: Solving The Chess Grandmaster Problem, Saarland University, 2003

Amir, Y. (2006): The Insider Threat: A Challenge to Scalable Networked Systems. EU-US Summit Cyber trust: System Dependability & Security, 15.-16.11.2006, Dublin

Anderson, R. (2003): Cryptography and Competition Policy – Issues with 'Trusted Computing'. Annual ACM Symposium on Principles of Distributed Computing 2003

Anderson, R. (2006): Trusted Computing FAQ, in: http://moon,hipjoint.de/tcpa-palladium-faq-de.html, Abruf am 23.05.2007

Bechthold, S. (2003): Urheberrechtliche und institutionelle Risiken des Trusted Computing, Universität Tübingen, 2003

Bechthold, S. (2006): Rechtliche Technikgestaltung von Digital-Rights-Management-Systemen – ein Blick auf eine entstehendes Forschungsgebiet. Institut für Technikfolgenabschätzung und Systemanalyse (ITAS), in: http://www.itas.fzk.de/tatup/062/bech06a.htm, Abruf am 23.05.2007

Bechtold, R. (2006): Kartellgesetz, 4. A.

Bechtold, R. / Bringer, I. / Bosch, W. / Hirsbrunner, S. (2005): EG-Kartellrecht, Tübingen

Bechtold, S. (2005): Trusted Computing: Rechtliche Probleme einer entstehenden Technologie, in: Computer und Recht 6/2005, S. 393-404

Bechtold, S. (2004): Trusted Computing Initiatives – Protecting Virtual Troy or Creating a Tojan Horse?, in: Koenig, Ch. / Neumann, A. / Katzschmann, T. (Hrsg.): Trusted Computing, S. 77 – 99

Bechtold, S. (2005): Trusted Computing, CR 2005, 393 – 404

Becker, E., Buhse, W., Günnewig, D., Rump, N. (2003): Digital Rights Management. Technological, Economic, Legal and Political Aspects, 2003

Bethge, H. (2003): Zur verfassungsrechtlichen Legitimation informalen Staatshandelns der Bundesregierung, Jura, 327 – 333

Bitz, G. (2005): Informationsschutz im Unternehmen. Policy Enforcement mit Trusted Computing, in: Datenschutz und Datensicherheit (DuD) 29/2005, S. 531-536

Blaha, R. (2006): Trusted Computing auf dem Prüfstand des kartellrechtlichen Missbrauchsverbotes

Bleich, H. (2007): Ausweiskontrolle im Web, in: Magazin für Computer Technik (c't), 12/2007, S. 72-75

Bloomfield, R. (2007): Security and Dependability. Second Workshop of the EU/US summit series on Cyber Trust: System Dependability & Security, 26.-27.4.2007, Illinois

Böhle, K. (2006): Digital Rights Management – Optionen der Technikgestaltung. Institut für Technikfolgenabschätzung und Systemanalyse (ITAS), in: http://www.itas.fzk.de/tatup/062/boeh06a.htm, Abruf am 23.05.2007

Böttger, M., Fox, D. (1997): Sicheres Booten, in: Müller, G., Pfitzmann, A. (Hg.): Mehrseitige Sicherheit in der Kommunikationstechnik: Verfahren, Komponenten, Integration, Bonn 1997, S. 309-324

Brandl, H. (2008): Trusted Computing Grundlagen, in: Pohlmann, N. / Reimer, H. (Hrsg.), Trusted Computing, S. 21 – 42

Brandl, H. (2007): Trusted Computing. Grundlagen, bisherige Anwendungen und Tools. Trusted Computing Workshop am Institut für IT-Sicherheit / FH Gelsenkirchen am 03.05.2007, in: http://teletrust.de/fileadmin/files/ag2/Handout_TC-WS_2-Brandl.pdf, Abruf am 20.06.2007

Brandl, H. (2005): Trusted Computing – Aktuelle Anwendungen. Welche Funktionen sind schon heute nutzbar? in: Datenschutz und Datensicherheit (DuD) 29/2005, S. 537-541

Brandl, H., (2004): Trusted Computing: The TCG Platform Module Specification, Infineon Technologies AG, München 2004

Brandl, H., Rosteck, T. (2004): Technik, Implementierung und Anwendung des Trusted Computing Group-Standards (TCG). Sichere Plattform ermöglichen neue Sicherheitsniveaus, in: Datenschutz und Datensicherheit (DuD) 28/2004, S. 529-538

Büllingen, F. (2007): Informations- und Telekommunikationstechnologien (ITK) im Energiesektor – Inkrementelle Modernisierung oder Paradigmenwechsel? Das Projekt eEnergy, in: WIK-Newsletter Nr. 67, Juni, S. 6-9

Büllingen, F. et al. (2000): Position und Chancen der deutschen IT-Sicherheitsindustrie im globalen Wettbewerb, Bad Honnef

Bundesamt für Sicherheit in der Informationstechnik (2007): Die Lage der IT-Sicherheit in Deutschland 2007, Bad Godesberg

Bundesamt für Sicherheit in der Informationstechnik (o. J.): Sichere Platform und Trusted Computing Group, in: http://www.bsi.bund.de/sichere_plattformen/trustcomp/ infos/tcgi.htm, Abruf am 14.03.2007

Bundesamt für Sicherheit in der Informationstechnik (o. J.): Trusted Computing, in: http://www.bsi.de/sichere_plattformen/trustcomp/infos/tcgi.htm, Abruf am 24.05.2007

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (o. J.): Tätigkeitsbericht 2005-2006, in: BFDI, S. 54-55

Bundeskriminalamt (2007): Bundeslagebild. Wirtschaftskriminalität 2006, September, Wiesbaden

Bundesministerium des Innern (2007): Eckpunktepapier „Trusted Computing“ der Bundesregierung, 4. September 2007

Bundesministerium für Bildung und Forschung (2003): BMBF fördert Standart für IT-Sicherheit, in: http://www.bmbf.de/_search/searchresult.php?URL=http%3A%2F%2Fwww.bmbf.de%2Fpress%2F964.php&QUERY=bmbf+und+f%F6rdert, Abruf am 24.05.2007

Bus, J. (2007): Secure, Resilient & Trusted ICT Infrastructures in ICT-FP7. Second Workshop of the EU/US summit series on Cyber Trust: System Dependability & Security, 26.-27.4.2007, Illinois

Computerzeitung (2006): Trusted Computing hat als rotes Tuch ausgedient, in: http://www.computerzeitung.de/loader?path=/articles/2006045/30859942_ha_CZ.html&art=/articles/2006045/30859942_ha_CZ.html&thes=&pid=ee54f3c7-0de1-40f5-bb23-2cfdf022aee5&page=1, Abruf am 14.03.2007

Deutscher Bundestag (2003): Antwort der Bundesregierung: Auswirkung des “Trusted Platform Module” und der Software “Palladium“, Drucksache 15/660, Berlin 2003

Dolle, W. (2005): „Die Technik hinter dem Trusted Computing der TCPA/TCG – Chance oder Bedrohung für Linux?“ Linux Tag am 23. Juni, Karlsruhe

Dolle, W., Nerb, M., Wegener, Ch. (2006): In den Kinderschuhen, in: Linux-Magazin 2006/12, o. Seitenangabe

Dolle, W., Wegener, Ch. (2006): Trusted Computing für Linux – Stand der Dinge, in: Linux-Magazin 04/06, S. 100

Douglas, T. (o. J.): Cybersecurity and Domestic Surveillance or Why Trusted Computing Shouldn’t Be: Agency, Trust and the Future of Computing, in: www.oii.ox.ac.uk/microsites/cybersafety/extensions/pdfs/papers/douglas_thomas.pdf, Abruf am 23.05.2007

Duncan, C. (2004): Digital Rights Management. Intrallect Ltd, Linglithgow 2004

Emmerich, V. (2006): Kartellrecht, 10. A.,

Engberg, S. (2006): Balancing Security & Privacy in Dynamic Wireless Networks. EU-US Summit Cyber Trust: System Dependability & Security, 15-16.11.2006, Dublin

Engberg, S. (2006): Changing Security paradigms. From Trusted to Trustworthy Computing. SecurIST (2006): Joint Workshop. Security & Dependability in Mobile and Wireless. Future Requirements in R&D. Joint SecurIST, Mobile and Wireless Workshop am 11.-12.05.2007, Brüssel

Fichtinger, B. (2007): Trusted Infrastructures for Identities. Diplomarbeit Fachhochschule Hagenberg, 2007

Gärtner, M. (2007): Workshop zu Trusted Computing im Behördenumfeld. Bundesamt für Sicherheit in der Informationstechnik, in: http://www.bsi.bund.de/presse/pressinf/-280207_trustcomp.htm, Abruf am 24.05.2007

Gaßner, S. (2006): Tücken der Freiheit. Mobile Security wird zum Prüfstein für IT-Manager, in: http://www.silicon.de/enid/druckfunktion/22063, Abruf am 14.09.2007

Gawlas, F., Meister, G. (2005): Interaktionen TPM und Smart Card. Kombinierte Lösungen zur Verbesserung von Datenschutz und Datensicherheit. In: Datenschutz und Datensicherheit (DuD) 29/2005, S. 517-520

Grimm, R. Bizer, J., Will, A. (2006): Privacy4DRM: Nutzer-und datenschutzfreundliches Digital Rights Management, in: Datenschutz und Datensicherheit (DuD) 30/2006, S. 69-73

Grimm, R., Puchta, S. (2006): Datenspuren bei der Nutzung von Digital Rights Management-Systemen (DRM), in: Datenschutz und Datensicherheit (DuD) 30/2006, S. 74-79

Günnewig, D., Sadeghi, A., Stüble, C. (2003): Trusted Computing ohne Nebenwirkungen. Spezifikation der Trusted Computing Group sinnvoll nutzbar, in: Datenschutz und Datensicherheit (DuD) 27/2003, S. 556-560

Günnewig, D., Sadeghi, A., Stüble, C. (2003): Trusted Computing Platform Alliance. Mythen, Wirklichkeit und Lösungswege, in: http://krypt.cs.uni-sb.de/download/papers/GuSaSt2003.pdf, Abruf am 22.05.2007

Günnewig, D., Sadeghi, A., Stüble, C., Ranneberg, K. (2004): Trusted Computing Platforms – Zur technischen und industriepolitischen Situation und Vorgehensweise, in: Koenig, C., Neumann, A., Katzschmann, T.(Hg.): Trusted Computing, Technik, Recht und gesellschaftspolitische Implikationen vertrauenswürdiger Systemumgebungen, Heidelberg 2004

Hansen, M. (2004): A Double–Edge Blade. On Trusted Computing's Impact on Privacy, in: Datenschutz und Datensicherheit (DuD) 28/2004, S. 525-528

Hansen, M. (2005): Privacy Dilemma of Trusted Computing. TCG's Pronciples and Demands from Privacy Authorities, in: Datenschutz und Datensicherheit (DuD) 29/2005, S. 542-543

Hansen, M. (2006): DRM-Desaster: Das Sony BMG-Rootkit. Dubiose DRM-Software unterwandert System-Sicherheit, in: Datenschutz und Datensicherheit (DuD) 30/2006, S. 95-97

Hansen, M., Pfitzmann, A. (2007): Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identitiy Management – A Consolidated Proposal for Terminology, in: http://dud.inf.tu-dresden.de/Anon_Terminology.ahtml, Abruf am: 11.08.2007

Hansen, M. / Hansen, M. (2007): Auswirkungen von Trusted Computing auf die Privatsphäre, in: Pohlmann, N. / Reimer, H. (Hrsg.), Trusted Computing, S. 209 – 220

Hariton, G., Palihapitya, H. (2006): Should Consumers Trust Trusted Computing? Public Interest Advocacy Centre, Ontario 2006

Hartel, P. (2007): Comparing Internet and Real World Security. Second Workshop of the EU/US summit series on Cyber Trust: System Dependability & Security von 26.-27.4.2007, Illinois

Hartmann, M. (2005): Trusted Network Connect. Netzwerkhygiene auf hohem Niveau, in: Datenschutz und Datensicherheit (DuD) 29/2005, S. 544-547

Hartmann, M. (2005): Trusted Web Services, in: Datenschutz und Datensicherheit (DuD) 29/2005, S. 160-162

Hartmann, M. (2007): Enterprise Rights Management. Trusted Computing Workshop am Institut für IT-Sicherheit / FH Gelsenkirchen am 03.05.2007, in: http://teletrust.de/fileadmin/files/ag2/Handout_TC-WS_4-Hartmann.pdf, Abruf am 20.06.2007

Heckmann, D. (2005): IT-Beschaffung der öffentlichen Hand zwischen Haushalts- und Marktpolitik, CR, 711 – 715

Heinemann, A. (2005): Kartellrecht und Informationstechnologie, CR, 715 – 720

Heise Online (2004): Bundesregierung veröffentlicht Positionspapier zu Trusted Computing, in: http://www.heise.de/newsticker/meldung/45516, Abruf am 20.03.2007

Heise Online (2004): WinHEC: NGSCB/Palladium im Wandel, in: http://www.heise.de/newsticker/ meldung/47139, Abruf am 20.03.2007

Heise Security (2003): Trusted Computing im Überblick, in: http://www.heise.de/security/artikel/print/43179, Abruf am 23.05.2007

Helmuth, C., Warg, A., Feske, N. (o. J.): Microkernel-Based Systems. Secure Systems Mikro-SINA and Nizza, TU Dresden, in: http://os.inf.tu-dresden.de/Studium/KMB/Folien/10-SecureSystems/10-SecureSystems.pdf, Abruf am 20.06.2007

Hottelet, U. (2003): Experten streiten über Trusted Computing. VDI Nachrichten, in: http://www.vdinachrichten.com/vdi_nachrichten/aktuelle_ausgabe/akt_ausg_detail.asp?source=volltext&cat=2&id=12998, Abruf am 20.03.2007

Huber, P. M. (2003): Die Informationstätigkeit der öffentlichen Hand- ein grundrechtliches Sonderregime aus Karlsruhe?, JZ, 290 – 297

Hüttner, T. (2006): Challenges in Enterprise Scale TPM + Key Management, in: http://www.teletrust.de/fileadmin/files/ag2/Handout_TC-WS_7-H_ttner.pdf, Abruf am 20.06.2007

IDG.net (2000): Microsoft in China: Clash of Titans, in: http://archives.cnn.com/2000/-TECH/computing/02/23/microsoft.china.idg/, Abruf am 23.05.2007

Jefferies, N. (2006): EMobility – Views of security from a technology platform. SecurIST: Joint Workshop. Security & Dependability in Mobile and Wireless: Future Requirements in R&D. Joint SecurIST, Mobile and Wireless Workshop am 11.-12.05.2007, Brüssel

Joseph, A. (2006): Designing and Testing Networked Embedded Control Systems. EU-US Summit Cyber Trust: System Dependability & Security, 15.-16.11.2006, Dublin

Jungbauer, M. (2007): Trusted Network Connect. Vertrauenswürdige Netzwerkverbindungen. Trusted Computing Workshop in Gelsenkirchen im Mai 2007, in: http://www.teletrust.de/fileadmin/files/ag2/Handout_TC-WS_5-Jungbauer.pdf, Abruf am 26.09.2007

Just, J. (2006): Testing the Effectiveness of Cyber-Defenses. EU-US Summit Cyber trust: System Dependability & Security, 15.-16.11.2006, Dublin

Kauer, B. (2007): OSLO: Improving the security of Trusted Computing. 16th Usenix Security Symposium 6. – 10.08.2007 in Boston, in: http://os.inf.tu-dresden.de/papers_ps/kauer07-oslo.pdf, Abruf am 03.09.2007

Kay, R. (2005): The Future of Trusted Computing, https://www.trustedcomputinggroup.org/home/IDC_Presentation.pdf

Kesidis, G. / Carl, G. (2006): Large Scale Routing Experimentation for Next-Generation Networking. EU-US Summit Cyber Trust: System Dependability & Security, 15.-16.11.2006, Dublin

Koenig, C. (o. J.): Trusted Computing im Fadenkreuz des EG-Wettbewerbsrechts, ZEI, Bonn

Koenig, C., Neumann, A., Katzschmann, T. (Hg.)(2004): Trusted Computing, Heidelberg, 2004

Koenig, Christian / Loetz, Sascha / Neumann, Andreas, (2003) Innovation im Spannungsverhältnis von Markt und Regulierung, in: Klumpp, D. / Kubicek, H. / Roßnagel, A. (Hrsg.): next generation information society? S. 403 – 412

Koenig, Ch. / Loetz, S. / Neumann, A. (2004): Telekommunikationsrecht

Koenig, Christian / Loetz, Sascha / Neumann, Andreas, Innovation im Spannungsverhältnis von Markt und Regulierung, in: Klumpp, D. / Kubicek, H. / Roßnagel, A. (Hrsg.)(2003): next generation information society? S. 403 – 412

Koenig, Ch. / Neumann, A. (2004): Neue wettbewerbspolitische und -rechtliche Entwicklungen zum „Trusted Computing“, DuD, S. 555 – 560

Koenig, Ch. / Neumann, A. (2004): Wettbewerbsrechtliche Aspekte vertrauenswürdiger Systemumgebungen, in: Koenig, Ch. / Neumann, A. / Katzschmann, T. (Hrsg.): Trusted Computing, S. 100 – 140

Koenig, Ch. / O'Sullivan, D. (2003): Is „Trusted Computing“ an Antitrust Problem?, ECLR, S. 449 – 457

Koenig, Ch. / Vogelsang, I. / Kühling, J. / Loetz, S. / Neumann, A. (2002): Funktionsfähiger Wettbewerb auf den Telekommunikationsmärkten

Koenig, Ch. (11/2006): EG-wettbewerbsrechtliche Grundstandards für Industriestandards", EWS (Editorial)

Kohler, T. (2006): Banking in 2015 and IST Impact on Technology, namely on Mobile Technology. Joint SecurIST, Mobile and Wireless Workshop am 11.-12.05.2007, Brüssel

Kommission, (2001): Interpretierende Mitteilung der Kommission über das auf das Öffentliche Auftragswesen anwendbare Gemeinschaftsrecht und die Möglichkeiten zur Berücksichtigung von Umweltbelangen bei der Vergabe öffentlicher Aufträge, KOM 274 endgültig

Kommission, (2001): Mitteilung der Kommission über die Auslegung des gemeinschaftlichen Vergaberechts und die Möglichkeiten zur Berücksichtigung sozialer Belange bei der Vergabe öffentlicher Aufträge, KOM 566 endgültig

Kopp, F. O. / Ramsauer, U. (2005): VwVfG, 9. A.

Kotz, D. (2006): Digital Living 2010: Sensors, Privacy, and Trust. EU-US Summit Cyber Trust: System Dependability & Security, 15.-16.11.2006, Dublin

Krempl, S. (2007): Bundesregierung debattiert über Trusted Computing, in: http://www.heise.de/security/news/meldung/print/85920, Abruf am 25.05.2007

Kuhlmann, D. (2004): Vertrauenssache Trusted Computing. Versuch einer Zwischenbilanz, in: Datenschutz und Datensicherheit (DuD) 28/2004, S. 545-547

Kung, A. (2006): Security in eSaftey Projects. SecurIST (2006): Joint Workshop. Security & Dependability in Mobile and Wireless: Future Requirements in R&D. Joint SecurIST, Mobile and Wireless Workshop am 11.-12.05.2007, Brüssel

Kuntze, N./ Schmidt U. (2006): Transitive trust in mobile scenarios. International Conference on Emerging Trends in Information and Communication Security, 6.-9. Juni, Freiburg

Kuntze, N./ Schmidt U. (2006): Trusted Computing in Mobile Action, Frauenhofer-Institut for Secure Information Technology SIT, Darmstadt 2006

Kuntze, N./ Schmidt U. (2007): Protection of Systems by Trusted Computing, Frauenhofer-Institut for Secure Information Technology SIT, Darmstadt 2007

Kuntze, N./ Schmidt, A. (2007): Trusted Ticket Systems and Applications, Frauenhofer-Institut for Secure Information Technology SIT, Darmstadt 2007

Kursawa, K./ Reimer, H. (2005): TC – Transparenz und Vertrauen? in: Datenschutz und Datensicherheit (DuD) 29/2005, S. 508

Lampson, B. (2006): Measuring Security? EU-US Summit Cyber Trust: System Dependability & Security von 15.-16.11.2006 Dublin

Lee, W. (2006): Security Infrastructure for Mobile Devices. EU-US Summit Cyber Trust: System Dependability & Security von 15.-16.11.2006, Dublin

Lemke, K., Paar, Ch., Wolf, M. (Hg.)(2006): Embedded Security in Cars – Securing Current and Future Automotive IT Applications, Berlin-NewYork-Hamburg

Lemos, R. (2006): Apple makes Trusted Computing cool, 2. August, www.securityfocus.com

Levitt, K. (2006): Computing in the 21st Century. Lifting Vision to Higher Sights. EU-US Summit Cyber Trust: System Dependability & Security, 15.-16.11.2006, Dublin

Linnemann, M. / Heibel, N. / Pohlmann, N. (2007): Mehr Vertrauenswürdigkeit für Anwendungen durch eine Sicherheitsplattform, in: Pohlmann, N. / Reimer, H. (Hrsg.), Trusted Computing, S. 73 – 85

Littlewood, B. (2006): 'Confidence' in Probability-based Dependability/Security Cases for the Support of Risk Assessment. EU-US Summit Cyber Trust: System Dependability & Security, 15.-16.11.2006, Dublin

Lomholt, F. (1998): The 1984 IBM Undertaking, Competition Policy Newsletter 3, S. 7 – 11

Madeira, H. (2006): "Beyond Test Beds." EU-US Summit Cyber Trust: System Dependability & Security, 15.-16.11.2006, Dublin

Markatos, E. (2006): Next generations threat on the Internet: Research challenges. EU-US Summit Cyber Trust: System Dependability & Security, 15.-16.11.2006, Dublin

Masera, M. (2006): The case of networked industrial systems. EU-US Summit Cyber Trust: System Dependability & Security, 15.-16.11.2006, Dublin

McHough, J. (2006): Thought on Evaluating the Dependability & Security of Networked Systems. EU-US Summit Cyber Trust: System Dependability & Security, 15.-16.11.2006, Dublin

Möller, J. (2006): Automatisiertes Management von Datenschutzrechten. Zum Einsatz von DRM jenseits der Urheberrechte, in: Datenschutz und Datensicherheit (DuD) 30/2006, S. 98-101

Möller, J., Bizer, J. (2006): Datenschutzanforderungen an Digital Rights Management. Rechtsdurchsetzung für Urheber und Verwerter kontra Datenschutz der Nutzer, in: Datenschutz und Datensicherheit (DuD) 30/2006, S. 80-84

Montari, U. / Sanella, D. / Bruni, R. (2007): Trustworthy Global Computing. Secon Symposium TCG 2006, Lucca Italy Nov. 2006. Revised selected papers, Berlin, Heidelberg

Müller, Th. (2007): Trusted Computing mit Windows Vista und Windows Server “Longhorn”, Vortrag 10. BSI-Kongreß, 22.-24. Mai, Bad Godesberg

Müller, U. / Meyer, L. (2007): Wettbewerb und Regulierung in der globalen Internetökonomie – Eine rechtsvergleichende Studie zwischen europäischem und US-amerikanischem Recht

Nanya, T. (2006): Japanese Research Initiative on Dependable Information Systems. EU-US Summit Cyber Trust: System Dependability & Security, 15.-16.11.2006, Dublin

Neumann, A. (2004): Trusted Computing und Wettbewerbsrecht – Entwicklung einer IT-Sicherheitsarchitektur unter den Bedingungen des EG-Kartellrechts. Vortrag im Workshop 3 (Regulierung und Selbstregulierung) bei der Jahrestagung 2004 der Deutschen Gesellschaft für Recht und Informatik e. V. am 8. Oktober 2004

Neumann, A. (2004): Trusted Computing. Sitzung des DIHK-Ausschusses „Telekommunikation und neue Dienste“ am 13. Mai 2004

Neumann, A., Koenig, C. (2004): Neue wettbewerbspolitische und –rechtliche Entwicklungen zum “Trusted Computing”, in: Datenschutz und Datensicherheit (DuD) 28/2004, S. 555-560

Neumann, A. (2005) Entwicklung einer IT-Sicherheitsarchitektur im Wege koordinativer Standardisierung, in: Taeger, J. / Wiebe, A. (Hrsg.), Mobilität Telematik Recht, S. 187 – 217

Neumann, A. (2008): Rechtliche Chancen und Risiken des „Trusted Computing“, in: Pohlmann, Norbert / Reimer, Helmut (Hrsg.), Trusted Computing, S. 221 – 236

Nixon, P. (2006): Trust is the Key. EU-US Summit Cyber Trust: System Dependability & Security, 15.-16.11.2006, Dublin

Obert, T. (2005): Next Generation Secure Computing Base. TPM Support mit Microsoft Vista (ehemals Longhorn), in: Datenschutz und Datensicherheit (DuD) 29/2005, S. 521-525

Ohler, Ch. (2002): Anmerkung zum Beschluss des BVerfG v. 26.6., ZLR 2002, S. 631 – 639

Paar, C., Pelzl, J., Schramm, K., Weimerskirch, A., Wollinger, T. (2004): Eingebettete Sicherheit: State-of-the-art. Escrypt, in: http://www.escrypt.com/escrypt_engl/download/dach2004_embedded_security_v6.pdf, Abruf am 30.07.2007

Palandt, O. (2007): Bürgerliches Gesetzbuch, 66. A.

Paxon, V. (2007): "Perspectives on International Network Security Research." Second Workshop of the EU/US summit series on Cyber Trust: System Dependability & Security von 26.-27.4.2007, Illinois

Pfitzner, R., Dix, A. (2003): Trusted Computing und Datenschutz in Deutschland, in: Datenschutz und Datensicherheit (DuD) 27/2003, S. 561-562

Pisko, E. / Rannenberg, K. / Roßnagel, H. (2005): Trusted Computing in Mobile Platforms. Payers, Usage Scenarios, and Interests, in: Datenschutz und Datensicherheit (DuD) 29/2005, S. 526-530

Plura, M. (2002): Der versiegelte PC. Magazin für Computer Technik (c't), in: http://www.heise.de/ct/02/22/204/, Abruf am 23.05.2007

Plura, M. (2002): Schlossgespenst. Magazin für Computer Technik (c't), in: http://www.heise.de/ct/02/26/054/, Abruf am 23.05.2007

Pohlmann, N. (2004): XKMS – TrustPoint, Institut für Internet-Sicherheit, in: http://www.internet-sicherheit.de/fileadmin/npo/artikel_berichte/XKMS-TrustPoint1.pdf, Abruf am 12.09.2007

Pohlmann, N. (2005): EMSCB – ein Überblick. Vortrag BITKOM-Arbeitskreis Sicherheitstechnologien, 5. Okt. 2005, Bonn

Pohlmann, N. (2007): Trusted Computing. Schnittstelle und Standards. Vortrag auf dem Trusted Computing Workshop, 19. Mai 2007, Gelsenkirchen

Pohlmann, N. (2007): TURAYA – An Open Trusted Computing Platform. Vortrag beim Round Table Meeting in Connection with the RSA-Conference, San Francisco 2007

Pohlmann, N. / Heibel, N. / Linnemann, M. (2007): Trusted Computing – Projekte, Erfahrungen und Piloten, Vortrag auf der CeBIT 2007, Hannover

Pohlmann, N. / Heibel, N. / Linnemann, M. (2007): TURAYA Anwendungsbeispiele – Projekte, Erfahrungen und Piloten, Vortrag auf der CeBIT 2007, Hannover

Pohlmann, N. / Jungbauer, M. (2006): Vertrauenswürdige Netzwerkverbindungen mit Trusted Computing. Sicher vernetzt? in: IT-Sicherheit, 6/2006, S. 46-47

Pohlmann, N. / Linnemann, M. (2007): TURAYA – Die offene Trusted-Computing-Sicherheitsplattform, in: http://www.internet-sicherheit.de/fileadmin/npo/artikel_berichte/TURAYA-Die-offene-Trusted-Computing-Sicherheitsplattform.pdf, Abruf am 12.09.2007

Pohlmann, N. / Reimer, H. (Hrsg.)(2008): Trusted Computing. Ein Weg zu neuen IT-Sicherheitsarchitekturen, Wiesbaden

Pohlmann, N. / Sadeghi, A. / Stüble, C. (2004): European Multilateral Secure Computing Base. Open Trusted Computing for You and Me, in: Datenschutz und Datensicherheit (DuD) 28/2004, S. 548-554

Rannenberg, K. (2006): Duality between digital privacy and collective security: digital dignity and sovereignty. SecurIST Networking Session am 22.11.2006, Helsinki

Reid, J. / Caelli, W. (2005): DRM, Trusted Computing and Operating System Architecture, Australasian Information Security Workshop 2005, Newcastle, Australia, 2005

Reimer, H. / Linnemann, M. (2007): Trusted Computing Whitepaper, TeleTrusT Deutschland e.V.. Erfurt 2007

Reiter, M. (2007): Trustworthy Services. Second Workshop of the EU/US summit series on Cyber Trust: System Dependability & Security, 26.-27.4.2007, Illinois

Ritscher, M. (2007): Sicherheit des mobilen Büros – Ein Überblick, Vortrag auf dem "Secure Mobile Computing" KompetenzTag des TelekomForums am 15.10.2007, Bonn

Sadeghi, A. (2007): The need and Challenges for Trusted Computing, Horst Görtz Institute for IT Security Ruhr-University Bochum, 2007

Sadeghi, A. / Selhorst, M. / Senft, O. / Stüble, C. / Winandy M. (2005): New Aspects on Trusted Computing. New and Advanced Possibilities to Improve Security and Privacy, in: Datenschutz und Datensicherheit (DuD) 29/2005, S. 511-516

Sailer, R. / Doorn, L. van / Ward, J. (2004): The Role of TPM in Enterprise Security, in: Datenschutz und Datensicherheit (DuD) 28/2004, S. 539-544

Sanders, W. (2006): Evaluating the Dependability & Security of networked Systems – Modelling, Simulation, Predictive Evaluation, Assurance Cases. EU-US Summit Cyber trust: System Dependability & Security, 15.-16.11.2006, Dublin

Sandl, U. (2004): Die Trusted Computing Group (TCG). Eine Herausforderung auch für die deutsche Wirtschaftspolitik, in: Datenschutz und Datensicherheit (DuD) 28/2004, S. 521-524

Saydjari, S. (2006): Measuring Risk. EU-US Summit Cyber trust: System Dependability & Security, 15.-16.11.2006, Dublin

Schallbruch, M. (2004): Trusted Computing – Chance für eine sichere Informationsgesellschaft? Vertrauen in sichere Informationstechnik, in: Datenschutz und Datensicherheit (DuD), 28/2004, S. 519-520

Schoen, S. (o. J.): Trusted Computing: Promise and Risk. Electronic Frontier Foundation, in: http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.php, Abruf am 23.05.2007

SecurIST Advisory Board (2007): Recommendations for a Security and Dependability Research Framework: From Security and Dependability by Central Command and Control to Security and Dependability by Empowerment, Brussels 15. Januar

Silicon (2006): Mobile Sicherheit. Trusted Computing Group stellt Standard für Headsets vor, in: http://www.silicon.de/enid/antivirus/22321, Abruf am 14.09.2007

Skordas, T. (2006): Secure, Resilient & Trusted ICT Infrastructures RTD Funding Opportunities in the EU`s ICT-FP7. EU-US Summit Cyber trust: System Dependability & Security, 15.-16.11.2006, Dublin

Speilkamp, M. (2006): Was kaufe ich im Online-Musikgeschäft? DRM und seine (mangelnde) Transparenz für den Kunden, in: Datenschutz und Datensicherheit (DuD) 30/2006, S. 90-94

Stallman, R. (2002): Can You Trust Your Computer? in: http://slash.autonomedia.org /article.pl?sid=02/10/26/2315242&mode=nested, Abruf am 22.05.2007

State Services Commission (2006): Trusted Computing and Digital Rights Management Principles & Policies, New Zealand, 2006

Stewen, T. (2004): Trusted Computing & Digital Rights Management – Theory & Effects, Växjö University, Växjö 2004

Stumpf, F. / Sacher, M. / Roßnagel, A. / Eckert, C. (2007): Erzeugung elektronischer Signaturen mittels Trusted Platform Module, in: Datenschutz und Datensicherheit (DuD) 31/2007, S. 357-361

Suri, N. (2006): A Line in the Sand: Securing an Increasingly Insecure Environment. EU-US Summit Cyber trust: System Dependability & Security, 15.-16.11.2006, Dublin

TeleTrusT (2007): Trusted Computing Whitepaper, Erfurt

Trusted Computing Group (2005): Embedded Systems and Trusted Computing Security. Trusted Computing Group, in: https://www.trustedcomputinggroup.org/groups/tpm/embedded_bkgdr_final_sept_14_2005.pdf, Abruf am 24.05.2007

Trusted Computing Group (2005): Trusted Platform Modules Strengthen User and Platform Authenticity January 2005, in: https://www.trustedcomputinggroup.org/specs/TPM/Whitepaper_TPMs_Strengthen_User_and_Platform_Authenticity_Final_1_0.pdf, Abruf am 25.05.2005

Trusted Computing Group (2007): Trusted Computing Group Frequently Asked Questions May 2007, in: https://www.trustedcomputinggroup.org/faq/, Abruf am 24.05.2007

Tsudik, G. (2006): Some Security & Privacy Challenges in Wireless/Mobile Networks. EU-US Summit Cyber trust: System Dependability & Security, 15.-16.11.2006, Dublin

Ullrich, Hanns, Patente, (2007): Wettbewerb und technische Normen: Rechts- und ordnungspolitische Fragestellungen, GRUR, S. 817 – 830

Varian, H. (2000): Managing Online Security Risks, in: http://www.ischool.berkley.edu/~hal/people/hal/NYTimes/2000-06-01.html, Abruf am 30.05.2007

Vaslin, R. / Gogniat, G. / Diguet, J. / Pegatoquet, A. (2007): Trusted Computing. A New Challenge for Embedded Systems. IEEE 13th International Conference on Electronics, Cicuits and Systems 2007, Nice, Frankreich 2006

Verissimo, P. (2006): Embedded systems pave the road to the future Internet. EU-US Summit Cyber trust: System Dependability & Security, 15.-16.11.2006, Dublin

Weimerskirch, A. / Paar, Ch. / Wolf, M. (o. J.): Komponentenidentifikation: Voraussetzung für IT-Sicherheit im Automobil, Bochum

Weis, R. (2004): DRM und “Trusted Computing“. Cryptolabs, Amsterdam 2004

Weis, R. (2004): Trusted Computing: Chancen und Risiken, in: Datenschutz und Datensicherheit (DuD) 28/2004, S. 651-654

Weis, R. / Bogk, A. (2004): Trusted Computing - eine unendliche Geschichte, in: http://www.ccc.de/congress/2004/fahrplan/files/247-WeisBogkTCunendlichCCC2004.pdf, Abruf am 02.05.2007

Will, A. / Jazdezejewski, S. / Weber, A. (2006): Kundenfreundlichkeit von Musik-Downloadplattformen? Ergebnisse aus der Studie Privacy4DRM, in: Datenschutz und Datensicherheit (DuD) 30/2006, S. 85-89

Winkler, D. (2007): Kommunale Gemeinwohlverantwortung, KommJur, S. 330 – 334

Wolf, M. (2007): Embedded Systems: Trusted Computing for Automobiles. Trusted Computing Workshop, Gelsenkirchen, 2007

Wollinger, Th. (2007): Embedded Systems. Trusted Computing im Automobil, Vortrag auf der CeBIT, 19. März in Hannover

Ziekow, J. (2007): Das Vergaberecht als Waffe gegen Kinderarbeit? KommJur, S. 281 – 288

Anhang

Fragebogen zu Trusted Computing

Industriepolitische Auswirkungen von „sicheren IT-Plattformen“ auf der Basis der „Trusted Computing“ (TC) Technologie

Projekt im Auftrag des Bundesministeriums für Wirtschaft und Technologie (BMWi)

WIK-Consult wurde vom BMWi beauftragt, eine Untersuchung zur o. g. Themenstellung durchzuführen. Hierbei spielt die Erhebung der Meinung und Einschätzungen des in Deutschland vorhandenen Expertenwissens eine zentrale Rolle für den Erfolg des Projektes. Wir bitten Sie vor diesem Hintergrund, an der Beantwortung der unten aufgeführten Fragen mitzuwirken.

Ausgangssituation

Seit Ende der 90er Jahre gibt es Aktivitäten der Industrie, den Umgang mit Computern sowie die Kommunikation über offene Netzwerke sicherer zu machen. Reine Softwarelösungen werden als nicht ausreichend betrachtet, für die erforderliche Sicherheit zu sorgen. Vielmehr soll durch den Einbau einer Hardware-Komponente (Trusted Platform Modul (TPM)) ein sicherer physischer Anker geschaffen werden, mit dessen Hilfe es möglich würde, Systemveränderungen zu messen, um darauf aufbauend eine Sicherheitskette zu generieren, die bis hin zu den Anwendungen reicht.

Seit 2003 hat die Trusted Computing Group (TCG) hierzu Standards entwickelt. Trotz verschiedener Anpassungen dieser Standards ist der Einbau von TPMs umstritten und es sind im Verlauf der letzten Jahre von unterschiedlicher Seite zahlreiche Kritiken vorgebracht worden. Trotzdem werden heute TPMs bereits millionenfach verbaut. Es gilt daher im Rahmen des Projektes herauszufinden, wie

- der aktuelle Stand der Entwicklung bei Trusted Computing (TC) beurteilt wird,
- welche die relevanten Akteure (in Deutschland; international) und ihre Positionen sind,
- welche Strategien im Bereich F&E, bei der Standardisierung und auf politischer Ebene erkennbar sind,
- wie diese Strategien verbessert werden können,
- wie den kritischen Einwänden (technisch, ökonomisch, wettbewerblich, datenschutzrechtlich, verbraucherpolitisch) begegnet wird,
- welche Entwicklungen mittelfristig wahrscheinlich sind,

- welche technischen Alternativen verfolgt werden,
- welche Szenarien längerfristig möglich bzw. wünschbar sind,
- welche Gestaltungs- und Handlungsoptionen auf nationaler, europäischer und internationaler Ebene bestehen in Hinblick auf die Politik, die Wirtschaft und die Forschung.

Um hierzu Informationen zu gewinnen und ein möglichst vollständiges Bild zeichnen zu können, sind die folgenden Fragen zu beantworten:

1. Fragen zur allgemeinen und politischen Gestaltung von TC

1.1 Sehen Sie mit der Einführung von TC / TPM tendenziell eher Chancen oder Risiken verbunden?

1.2 Wie würden Sie die künftige Entwicklung von TC beurteilen, wenn Sie in Kategorien eines Trendszenarios, also der Fortschreibung der aktuellen Entwicklung denken?

1.3 Welche Chancen, welche Risiken sehen Sie in Hinblick auf technische, ökonomische, wettbewerbliche, datenschutzrechtliche sowie verbraucherpolitische Fragestellungen?

1.4 Welche Handlungserfordernisse und Handlungsmöglichkeiten sehen Sie für sich sowie für andere Akteure (politische, industrielle), um TC zu gestalten und zu verbreiten?

1.5 Welche Erklärung sehen Sie, dass etwa ab 2004 die öffentliche Diskussion um TC beinahe zum Erliegen gekommen ist? Welche Entwicklungen sind für Sie seither erkennbar?

1.6 Nationale Alleingänge sind bei TC-Lösungen kaum Erfolg versprechend. Wie beurteilen Sie die Standardisierungserfordernisse auf europäischer bzw. internationaler Ebene? Welche Rollen spielen hierbei die ITU, ISO, WTO?

1.7 Welche Ansätze für eine gemeinsame deutsche / europäische Strategie bezüglich TC sind Ihnen bekannt? Halten Sie diesen Ansatz bzw. diese Ansätze für ausreichend?

1.8 Welche Notwendigkeiten und Chancen sehen Sie in einer Vernetzung aller bundesdeutschen TC-Akteure (Forschung, Unternehmen, Verbände, Politik)?

1.9 Wie sollte eine solche Vernetzung nach Ihrer Meinung konkret gestaltet sein?

1.10 Sind Ihnen Aktivitäten für eine nationale Vernetzung der Akteure bekannt?

1.11 In welchen Ländern befasst sich nach Ihren Erkenntnissen die Politik mit der TC-Technologie? Worin besteht deren Zielsetzung? Wie beurteilen Sie deren Chancen?

1.12 Wie beurteilen Sie die Aktivitäten der TCG?

2. Fragen zu F&E

2.1 Welche Universitäten oder sonstigen Forschungseinrichtungen beschäftigen sich in Deutschland mit sicheren Plattformen (insbesondere mit TC) bzw. der Entwicklung von TPMs?

2.2 Befassen Sie sich mit der Entwicklung von sicheren Plattformen (insbesondere der TC-Technologie)?

2.2.1 Wenn ja: Was sind die spezifischen Charakteristika Ihres Entwicklungsansatzes? Worin unterscheidet sich Ihr Ansatz gegenüber anderen Ihnen bekannten Entwicklungen?

2.2.2 Ist Ihr Projekt eigenfinanziert oder erhalten Sie Drittmittel?

2.2.3 Welche Marktchancen räumen Sie Ihrer Entwicklung ein?

2.2.4 Spielt die Frage der Interoperabilität bei Ihrem Ansatz eine Rolle?

2.2.5 Wo sehen Sie Markthemmnisse, wo sehen Sie Treiber für die Entwicklung und Verbreitung von TC allgemein?

2.3 Wie beurteilen Sie die bestehenden Möglichkeiten des Zugangs zu Informationen über aktuelle technische Entwicklungen auf der Ebene der TCG und anderer Institutionen / Unternehmen mit einer Schlüsselposition in diesem Bereich? Wie beurteilen Sie die Möglichkeit bzw. das Interesse, sich in entsprechende Projektentwicklungen der Industrie einzubringen?

2.4 Wo sehen Sie Notwendigkeiten für weitere F&E-Aktivitäten? Haben Sie konkrete Projektideen, für die Sie eine Finanzierung für sinnvoll erachten?

2.5 Wo liegen die Schwerpunkte dieser Ideen, wie schätzen Sie deren Realisierungschancen ein, welchen Zeitraum würden diese Aktivitäten benötigen? Sehen Sie Chancen oder Notwendigkeiten einer Kooperation mit anderen Forschungsakteuren?

2.6 Welche Rolle könnte Ihr Ansatz für eine nationale Sicherheitspolitik spielen?

2.7 Wenn alternative Forschungsansätze existieren, wie beurteilen Sie deren Realisierungschancen?

2.8 Sehen Sie Möglichkeiten einer Vernetzung auf der Ebene von F&E? Sind Ihnen Aktivitäten für eine solche Vernetzung bekannt? Wer sollte hier initiativ werden?

2.9 Wie beurteilen Sie die Rolle der TC/TPM-bezogenen Forschung in Deutschland im Vergleich zu anderen Ländern?

2.10 In welchen Ländern sind nach Ihrer Einschätzung besonders wichtige, besonders Ressourcen-intensive oder besonders brisante F&E-Aktivitäten zu beobachten?

2.11 Welche Projekte kennen Sie in Deutschland, die sich mit sicheren Plattformen (insbesondere der TC-Technologie) unter Nutzung von TPM befassen?

2.11.1 Von wem werden diese Projekte durchgeführt bzw. gefördert?

2.11.2 Welche sind die Motive für die Entwicklung dieser Projekte?

2.11.3 Wie ist der Stand der Entwicklung dieser Projekte?

2.11.4 Was sind die besonderen Charakteristika dieser Projekte, über welche besonderen Eigenschaften verfügen sie?

2.11.5 Wie bewerten Sie deren Marktperspektiven?

2.11.6 Welche Vorteile sind für die Anbieter, welche für Anwender damit verbunden?

2.12 Besteht eine Wettbewerbssituation zwischen den unterschiedlichen Lösungen? Wie würden Sie deren Chancen für ihre Durchsetzung beurteilen?

3. Fragen zur Rolle der Verbände

3.1 Welche Rolle spielt TC in Ihrem Verband? Welche Aktivitäten verfolgen Sie?

3.2 Welche Rolle können / sollten Verbände in der Diskussion um TC spielen? Wissen Sie, ob entsprechende Aktivitäten geplant sind?

3.3 Wie beurteilen Sie die Notwendigkeit einer Koordination und Vernetzung der nationalen TC-Aktivitäten? Welche institutionellen und organisatorischen Lösungen erscheinen aus Ihrer Sicht sinnvoll und nachhaltig?

4. Industriepolitische Fragestellungen

4.1 Welche Auswirkungen wird TC aus Ihrer Sicht auf die Verbreitung und Nutzung quelloffener Software (OSS) haben?

4.2 Deutsche Unternehmen wirken in der TCG mit. Wie beurteilen Sie diese Aktivitäten und welche Erwartungen haben Sie? Sehen Sie die Interessen insbesondere von kleinen und mittleren Unternehmen dort hinreichend vertreten?

4.3 Was waren für Ihr Unternehmen die Gründe, sich für bzw. gegen eine Beteiligung in der TCG zu entscheiden?

4.4 Welche Unternehmen bzw. Branchen sehen Sie als die stärksten Promotoren der TC-Technologie an?

4.5 Welche Verbesserungsvorschläge haben Sie in Bezug auf die Arbeit der TCG oder lehnen Sie deren Arbeit ab?

4.6 Welche Chancen, welche Risiken sehen Sie in Hinblick auf die deutsche Software-Industrie, die Hardware-Hersteller, die Anwender?

4.7 Welche Handlungserfordernisse und Handlungsmöglichkeiten sehen Sie, um TC zu verbreiten?

4.8 Welche Konsequenzen erwarten Sie für die Entwicklung bzw. den Vertrieb von TC-Produkten angesichts etwaiger Patente, die bei der Implementierung von TC-Technologie berührt würden?

4.9 Was hielten Sie davon, wenn jeder potentielle Anbieter von TC-Produkten alle erforderlichen Lizenzen über einen zentralen „Technologiepool“ erhalten könnte? Wie müsste eine solche Einrichtung ggf. ausgestaltet sein?

4.10 Wie beurteilen Sie die Rolle der politischen Institutionen in Deutschland im Bereich TC? Welche Erwartungen haben Sie an die Politik?

4.11 Welche Unternehmen profitieren aus Ihrer Sicht am meisten von TC?

4.12 Welche Marktchancen erwarten Sie für Ihr Unternehmen hinsichtlich TC?

4.13 Wie beurteilen Sie das Potenzial der TC-Technologie zur Errichtung von Marktschranken?

4.14 Wie sehen Sie die deutsche IT-Sicherheitsindustrie in Bezug auf TC-Technologie positioniert?

4.15 Wie sehen Sie die Entwicklung von Trusted Network Connect (TNC)-Spezifikationen und der proprietären Alternativen (z. B. Microsoft Network Access Protection (NAP) oder Netzwork Admission Control (NAC) von Cisco)? Wie beurteilen Sie die möglichen Marktchancen dieser Techniken?