BEITRÄGE

CHRISTIAN KOENIG / ANDREAS NEUMANN

Anforderungen des EG-Wettbewerbsrechts an vertrauenswürdige Systemumgebungen

TCPA, TCG, Palladium und NGSCB

Unter dem Stichwort „Trusted Computing" wird derzeit ein technisches Konzept diskutiert, das die Computerindustrie sowie nachgelagerte Märkte der Unterhaltungs- und Medienwirtschaft nachhaltig verändern könnte. Ausgehend von einer Spezifikation, die von einer Gruppe führender Hard- und Softwarehersteller erarbeitet wurde, soll durch die Einführung vertrauenswürdiger Rechnerplattformen vornehmlich die Sicherheit technischer Systeme erhöht werden. Hierdurch ist aber die Herausbildung eines faktischen Standards zu erwarten, der wettbewerbliche Auswirkungen auf eine Vielzahl von Märkten haben wird. Gleiches gilt für die geplante Entwicklung eines vertrauenswürdigen Betriebssystems durch das Unternehmen Microsoft. Der nachfolgende Beitrag stellt die Technologie vertrauenswürdiger Systemumgebungen vor und skizziert die Anforderungen, die bei ihrer Markteinführung aus Sicht des EG-Wettbewerbsrechts erfüllt werden müssen.

I. Das Konzept vertrauenswürdiger Systemumgebungen

Obwohl das Thema „Trusted Computing" erhebliches Interesse der Fachöffentlichkeit erregt hat,[1] Anlass mehrerer parlamentarischer Anfragen[2] und allein in Deutschland auch bereits Thema zweier rechtswissenschaftlicher Fachkonferenzen[3] war, sind die technischen Hintergründe dieses neuen Konzepts kaum bekannt. Nachfolgend werden daher zunächst das grundlegende Konzept vertrauenswürdiger[4] Rechnerplattformen (unter 1.)[5] sowie die geplante Implementierung eines vertrauenswürdigen Betriebssystems durch das Unternehmen *Microsoft* (unter 2.)[6] erläutert. Daran anschließend wird kurz dargestellt, welche praktischen Anwendungsmöglichkeiten die Verwendung vertrauenswürdiger Systemumgebungen eröffnet (unter 3.). Dabei soll der Begriff „vertrauenswürdige Systemumgebung" vertrauenswürdige Rechnerplattformen und darauf aufsetzende vertrauenswürdige Betriebssysteme zusammenfassen.

1. Vertrauenswürdige Rechnerplattformen

Computerviren, Schadprogramme, aber auch sonstige Manipulationen haben in den letzten Jahren der Öffentlichkeit vor Augen geführt, dass der zunehmende Einsatz von Computerprogrammen auch erhebliche Risiken mit sich bringt. Insbesondere hat sich zunehmend die Erkenntnis durchgesetzt, dass Systemsicherheit auf Programmebene allein nur sehr unvollkommen gewährleistet werden kann.[7] Vor diesem Hintergrund gründeten fünf namhafte Unternehmen der Hard- und Softwareindustrie[8] Anfang 1999 ein Industriekonsortium, das die Förderung des Vertrauens in Rechnerplattformen und -umgebungen zum Ziel hatte – die sog. *Trusted Computing Platform Alliance* (*TCPA*).[9] Vertrauenswürdig in dem dabei zu Grunde gelegten Sinne ist eine Systemkomponente dann, wenn sie sich stets in der erwarteten Weise hinsichtlich des verfolgten Zwecks verhält. Mittlerweile hat die *TCPA* technische Spezifikationen erarbeitet und beschlossen, die eine vertrauenswürdige Rechnerplattform definieren.[10] Die Spezifikationen fokussieren derzeit noch stark auf herkömmliche

---

1) S. nur *BITKOM*, Erläuterungen: Trusted Computing Platform Alliance (TCPA), im WWW abrufbar unter: http://www.bitkom.org. S. des Weiteren die Beiträge in *Koenig/Neumann/Katzschmann* (Hrsg.), Vertrauenswürdige Systemumgebungen, 2003 (i.E.), m.w.Nw.

2) BT-Drs. 15/116, S. 18; BT-Drs. 15/660.

3) Die erste wurde am 9.5.2003 vom *ZEI* in Zusammenarbeit mit *artikel5.de* und der *Microsoft Deutschland GmbH* durchgeführt – vgl. hierzu *Katzschmann*, K&R 2003, 347 –, die zweite am 2./3.7.2003 vom *BMWA* – vgl. hierzu *Himmelein*, c't 15/2003, S. 20.

4) Wenn im Folgenden der Begriff der Vertrauenswürdigkeit verwendet wird, wird damit lediglich auf das selbst gesetzte Ziel der Verfechter des „Trusted Computing" Bezug genommen. Eine wertende Aussage über die tatsächliche Vertrauenswürdigkeit entsprechender Systeme soll damit nicht verbunden sein.

5) Die Ausführungen zu den technischen Hintergründen vertrauenswürdiger Rechnerplattformen beruhen, ohne dass dies nachfolgend explizit ausgewiesen ist, auf *Pearson* (Hrsg.), Trusted Computing Platforms, 2003; *Pfitzner*, TCPA, Palladium und DRM – Technische Analyse und Aspekte des Datenschutzes, Stand: Juni 2003; *TCPA*, TCPA Design Philosophies and Concepts, Version 1.0; *dies.*, TCPA Specification/TPM Q&A, Stand: 16.10.2002. Der Artikel von *Pfitzner* ist abrufbar unter: http://www.lda.brandenburg.de/material/tcpa.pdf. Die „Design Philosophies" und die „Specification/TPM Q&A" sind seit kurzem nicht mehr über die WWW-Seite der *TCPA* abrufbar.

6) Die Darstellung der geplanten Entwicklung eines vertrauenswürdigen Betriebssystems durch *Microsoft* beruht auf *Pfitzner* (o. Fußn. 5) sowie auf den von *Microsoft* veröffentlichten Informationen, abrufbar unter: http://www.microsoft.com/resources/ngscb/productinfo.mspx.

7) S. hierzu etwa *Arbaugh/Farber/Smith*, A Secure and Reliable Bootstrap Architecture, in: Proceedings 1997 IEEE Symposium on Security and Privacy, S. 65.

8) Es handelte sich um *IBM*, *Intel*, *Microsoft* und die mittlerweile fusionierten Firmen *Compaq* und *Hewlett-Packard*. Anfang 2003 gehörten mehr als 200 Unternehmen der *TCPA* an.

9) Die WWW-Seite der *TCPA* ist abrufbar unter: http://www.trustedcomputing.org.

10) Version 0.90 der *TCPA*-Spezifikationen wurde im August 2000 veröffentlicht. Die zum Zeitpunkt des Manuskriptschlusses (Juli 2003) aktuelle Version 1.1b vom 22.2,2002 kommt auf eine Länge von über 300 Seiten. Die Version 1.2 wird gegenwärtig auf betroffene gewerbliche Schutzrechte überprüft und soll noch im Jahr 2003 verabschiedet werden, ist derzeit aber noch nicht veröffentlicht und kann daher nachfolgend auch nicht berücksichtigt werden.

Univ.-Prof. Dr. Christian Koenig ist Direktor am Zentrum für Europäische Integrationsforschung (ZEI) an der Universität Bonn. Andreas Neumann ist dort wissenschaftlicher Mitarbeiter. Die zitierten WWW-Seiten wurden zuletzt am 6.10.2003 überprüft. Die Verfasser danken Denis O'Sullivan, Jens-Daniel Braun, Sascha Loetz und Dr. Stefan Bechtold für ihre wertvollen Hilfestellungen zu diesem Beitrag.

Computersysteme (PCs), woran auch nachfolgend angeknüpft werden soll. Grundsätzlich ist das technische Konzept aber praktisch auf alle technischen Geräte übertragbar, die über Rechenprozesse gesteuert werden. Insbesondere könnten also auch PDAs,[11] Mobiltelefone und sogar Geräte der Unterhaltungselektronik (Video- und DVD-Abspielgeräte, Set-Top-Boxen etc.) zu vertrauenswürdigen Rechnerplattformen werden.[12]

Eine vertrauenswürdige Rechnerplattform besteht aus dem sog. Trusted Platform Module (TPM), dem Core Root of Trust for Measurement (CRTM) und dem Trusted Platform Support Service (TSS). Herzstück des Konzepts ist dabei das TPM,[13] ein Hardwaresicherheitsmodul, das fest an eine Rechnerplattform gebunden ist. Als CRTM wird die Software bezeichnet, die unmittelbar nach Systemstart ausgeführt wird – und damit in jedem Falle vor möglicherweise manipulierter Software. Der TSS schließlich bildet die Schnittstelle zwischen dem TPM und sämtlicher Software. In der praktischen Implementierung wird erwartet, dass das TPM regelmäßig den CRTM und den TSS beinhalten wird.

Das TPM erfüllt im Wesentlichen drei Funktionen.[14] Zunächst stellt es ein einzigartiges Schlüsselpaar zur Verfügung (Authentifizierungsfunktion), die sog. Endorsement Keys. Mit Hilfe dieser Schlüssel können weitere Schlüssel, die sog. Attestation Identity Keys erzeugt werden. Von diesen wiederum kann nicht auf die Endorsement Keys und damit auch nicht auf die jeweilige Rechnerplattform geschlossen werden. Sie begründen somit pseudoanonyme Identitäten, die u.a. zur Kommunikation mit Dritten, wie z.B. Anbietern im elektronischen Handel, verwendet werden können.

Des Weiteren stellt das TPM anderen Systemkomponenten kryptographische Funktionen zur Verfügung (Kryptographiefunktion). Dabei wird eine Schlüsselhierarchie erzeugt, die auf dem sog. Storage Root Key aufbaut, einem weiteren im TPM geschützten Schlüssel. Jeder dieser Schlüssel kann an einen bestimmten Systemzustand gebunden werden. In diesem Fall ist eine Entschlüsselung der mit einem solchen Schlüssel verschlüsselten Daten nur möglich, wenn sich das System in demselben Zustand wie zum Zeitpunkt der Verschlüsselung befindet.

Darüber hinaus dient das TPM der Überwachung des Systemzustands (Überwachungsfunktion), indem es Informationen zum Systemzustand speichert und über sie Auskunft erteilt. Diese Informationen werden dabei in bestimmten Registern abgelegt, den sog. Platform Configuration Registers (PCRs). Besonders relevant wird diese Überwachungsfunktion beim sog. Trusted Boot, bei dem die Integrität des Startvorgangs kontrolliert wird. Wie auf dabei festgestellte Änderungen des Systemzustands reagiert wird, legt allerdings nicht das TPM fest, sondern wird von der mit dem TPM kommunizierenden Software entschieden – insbesondere also dem BIOS[15] oder dem Betriebssystem. Erst die Überwachungsfunktion ermöglicht die Schaffung vertrauenswürdiger Systemumgebungen. Ausgehend von dem CRTM kann eine „Kette der Vertrauenswürdigkeit" geknüpft werden, indem jedes Programm, das eine andere Software lädt und ausführt,[16] vorher mit Hilfe des TPM deren Integrität misst. Auf diese Weise können Manipulationen am System festgestellt werden. Entsprechen alle Messwerte dem erwarteten Zustand, dann ist die Systemintegrität jedoch nachgewiesen und die Systemumgebung mithin vertrauenswürdig.

Das geschilderte Konzept einer vertrauenswürdigen Rechnerplattform setzt voraus, dass bestimmte Einschätzungen zutreffend sind: So müssen die Endorsement Keys in jedem TPM wirklich einzigartig sein, muss das TPM den *TCPA*-Spezifikationen entsprechen, muss ein Attestation Identity Key wirklich zu einem TPM gehören und muss bekannt sein, welche Messwerte einer zu ladenden Software deren Integrität anzeigen. Diese Einschätzungen werden im Konzept vertrauenswürdiger Systemumgebungen durch digitale Zertifikate bestätigt. Die *TCPA*-Spezifikationen definieren die Zuständigkeit für die Ausstellung dieser Zertifikate weitgehend abstrakt. Wer als Zertifizierungsinstanz – als sog. Certification Authority (CA) oder auch Trusted Third Party (TTP) – fungiert, wird für die einzelnen Zertifikate unterschiedlich und überdies auch uneinheitlich bestimmt werden können.[17] Diese Zertifizierungsinfrastrukturen bilden gewissermaßen ein in seiner Bedeutung kaum zu überschätzendes institutionelles Element vertrauenswürdiger Systemumgebungen.

Mittlerweile sind bereits die ersten *TCPA*-konformen Rechner erhältlich.[18] Zugleich wurde am 8.4.2003 die *Trusted Computing Group* (*TCG*)[19] als nicht gewinnorientierte Gesellschaft neu gegründet. Sie soll an die Stelle der *TCPA* treten und die *TCPA*-Spezifikationen weiterentwickeln sowie unterstützende Funktionen erfüllen.

2. Entwicklung eines vertrauenswürdigen Betriebssystems

Da eine vertrauenswürdige Rechnerplattform zunächst nur die hardwareseitigen Voraussetzungen für eine vertrauenswürdige Systemumgebung schafft, bedarf es insbesondere eines Betriebssystems, das diese Möglichkeiten nutzt. Zunächst unter dem Projektnamen „Palladium" und seit Anfang 2003 unter der Bezeichnung „Next-Generation Secure Computing Base" (NGSCB) plant derzeit das Unternehmen *Microsoft*, sein „Windows"-Betriebssystem um die hierfür notwendigen Funktionen zu erweitern. Nach den bisher bekannten Informationen soll die

---

11) Personal Digital Assistants (PDAs) sind Kleincomputer, die vor allem der Adress- und Terminverwaltung dienen, vgl. *Klußmann*, Lexikon der Kommunikations- und Informationstechnik, 3. Aufl. 2001, S. 757 f.

12) S. z.B. *Pfitzner* (o. Fußn. 5), S. 3; *TCG*, Frequently Asked Questions, Nr. 3. Die FAQ sind abrufbar unter: http://www.trustedcomputinggroup.org/about/faq/.

13) Bisweilen wird das TPM ironisch auch als „Fritz-Chip" bezeichnet, vgl. etwa *Anderson*, Upgrade 2003, Vol. 4 No. 3, 35, 36; *Microsoft*, Trustworthy Computing Initiative, Informationsblatt, Stand: Mai 2003, S. 3. Hiermit wird auf den US-Senator *Fritz Hollings* angespielt, der ein prominenter Befürworter von gesetzgeberischen Maßnahmen zum Schutz der Inhaber von Urheberrechten ist.

14) Eine etwas abweichende Klassifizierung findet sich bei *Pfitzner* (o. Fußn. 5), S. 4, sowie bei *TCG* (o. Fußn. 12), Nr. 19.

15) „Basic Input/Basic Output" (BIOS) bezeichnet die Software im nicht flüchtigen Speicher eines Computers, die beim Hochfahren des Systems abgearbeitet wird und die grundlegenden Systemfunktionen zur Verfügung stellt, vgl. *Klußmann* (o. Fußn. 11), S. 100 f.

16) Das CRTM überprüft also das BIOS, bevor es diesem die Kontrolle überträgt. Das BIOS überprüft dann das Ladeprogramm für das Betriebssystem, bevor es diesem die Kontrolle überträgt. Das Ladeprogramm wiederum überprüft das Betriebssystem, bevor es die Kontrolle an dieses weiterreicht.

17) So ist z.B. zu erwarten, dass eigene Konformitätsinstanzen („Conformance Entities" – CEs) bestätigen werden, dass eine TPM-Baureihe den *TCPA*-Spezifikationen entspricht. Auch ist abzusehen, dass regelmäßig der Hersteller eines TPM bestätigen wird, dass ein (öffentlicher) Endorsement Key zu diesem TPM gehört und dass zu der betreffenden TPM-Baureihe ein Konformitätszertifikat existiert. Weitaus unklarer ist derzeit jedoch insb. noch, wie die Zertifizierungsinfrastrukturen für die Attestation Identity Keys (durch sog. Privacy CAs) oder für die Integritätsmesswerte (durch sog. Validation Entities – VEs) praktisch ausgestaltet sein werden.

18) Vgl. etwa *BITKOM* (o. Fußn. 1), S. 1; *Bundesregierung*, BT-Drs. 15/795, S. 2; *Microsoft* (o. Fußn. 13), S. 4.

19) Die WWW-Seite der *TCG* ist abrufbar unter http://www.trustedcomputinggroup.org/.

NGSCB-Version von „Windows", die derzeit unter dem Projektnamen „Longhorn" entwickelt wird, hierzu insbesondere um einen sog. Trusted Operating Root erweitert werden, der als „Nexus" bezeichnet wird. Programme, Programmteile oder Dienste, die im Nexus laufen, werden dabei strikt von den anderen Bereichen des Betriebssystems abgeschirmt. Sie werden als „Nexus Computing Agents" (NCAs) bezeichnet. Herkömmliche sowie nicht auf das Konzept vertrauenswürdiger Systemumgebungen zugeschnittene Software kann unverändert im offenen Bereich des Betriebssystems ausgeführt werden. Die besondere Vertrauenswürdigkeit genießen jedoch nur die NCAs.

3. Vertrauenswürdige Systemumgebungen in der Anwendungspraxis

Die Anwendungsmöglichkeiten vertrauenswürdiger Systemumgebungen sind vielfältig und derzeit keinesfalls vollständig abzuschätzen. Vertrauenswürdige Systemumgebungen werden – etwa in Firmennetzwerken – dazu beitragen können, die Datensicherheit zu erhöhen. Des Weiteren werden sie die Authentifizierung von Transaktionen im elektronischen Handel erleichtern und können die Sicherheit der elektronischen Kommunikation erheblich steigern.

Indem in vertrauenswürdigen Systemumgebungen neue Möglichkeiten der Kontrolle des Zugangs zu digitalen Informationen bestehen, sind aber auch weniger populäre praktische Anwendungen denkbar. Zu nennen wäre hier vor allem die Implementierung von Systemen der digitalen Rechteverwaltung, also des sog. Digital Rights Managements (DRM).[20] Durch die Möglichkeit, die Nutzung von Inhalten von vorgegebenen Systemzuständen abhängig zu machen, könnte in einer vertrauenswürdigen Systemumgebung beispielsweise die Anfertigung von Kopien von Music-CDs oder von DVDs ausgeschlossen werden. Auf diese Weise ließen sich völlig neue Geschäftsmodelle verwirklichen, da bestimmte urheberrechtliche Verwertungsmodelle (z.B. Pay-per-View) nicht nur rechtlich, sondern technisch durchgesetzt werden könnten.[21]

II. Anforderungen des EG-Wettbewerbsrechts

Obwohl derzeit also noch ungewiss ist, in welcher Weise vertrauenswürdige Systemumgebungen später einmal tatsächlich genutzt werden, ergeben sich schon aus der Betrachtung des ihnen zu Grunde liegenden Konzepts zahlreiche rechtliche Fragestellungen. So berühren die aufgezeigten Möglichkeiten zur Implementierung weitreichender DRM-Systeme in erheblicher Weise urheberrechtliche Grundsatzfragen, wie namentlich das Recht auf Privatkopie.[22] Darüber hinaus kommt vertrauenswürdigen Systemumgebungen auch datenschutzrechtliche Relevanz zu.[23] Die nachfolgenden Ausführungen werden sich demgegenüber den Anforderungen an die derzeit erfolgende Etablierung technischer Standards für vertrauenswürdige Systemumgebungen zuwenden, die sich aus dem EG-Wettbewerbsrecht ergeben. Dabei sollen die institutionellen Aspekte[24] außer Betracht bleiben, da diese derzeit noch schwer abzuschätzen sind.[25]

1. Wettbewerbspolitische Implikationen der Standardisierung

Die wettbewerblichen Auswirkungen der Etablierung technischer Standards sind komplex und partiell gegenläufig.[26] Einerseits erhöhen Standards die Markttransparenz[27] sowie die Austauschbarkeit, die Kompatibilität und Interoperabilität von Gütern.[28] Die dadurch geschaffenen positiven Netzwerkeffekte wirken tendenziell sogar wettbewerbsfördernd.[29] Netzwerkeffekte sind andererseits aber ein zweischneidiges Schwert. Sie können auch zu Wettbewerbsbeschränkungen führen.[30] So können die von einer standardisierten Technologie ausgehenden Netzwerkeffekte als Marktzutrittsschranken für Wettbewerber wirken.[31] Dies kann auch den Innovationswettbewerb und die Vielfalt des Angebots beeinträchtigen.[32] Ähnliche Auswirkungen können sich durch Einsperrungseffekte („Lock-In") ergeben, wenn also durch Standards Pfadabhängigkeiten entstehen und Nutzer auf Grund hoher Wechselkosten vom Umstieg auf konkurrierende Technologien abgehalten werden.[33]

Die wettbewerbsrechtlichen Konsequenzen, die aus diesen komplexen ökonomischen Zusammenhängen zu ziehen sind, müssen nach der Art und Weise, in der ein technischer Standard etabliert wird, differenzierend betrachtet werden. Die Trennlinie läuft dabei weitgehend entlang der Unterscheidung zwischen der Standardisierung vertrauenswürdiger Rechnerplattformen durch die *TCPA/TCG*, die an Art. 81 EG zu messen ist (dazu unter 2.), und der einseitigen Etablierung technischer Standards für ein vertrauenswürdiges Betriebssystem durch das den Markt für PC-

---

20) S. etwa *Anderson*, Upgrade 2003, Vol. 4 No. 3, 35, 36; *Stallman*, Free Software, Free Society, 2002, S. 115 ff. Zum DRM vgl. grundlegend *S. Bechtold*, Vom Urheber- zum Informationsrecht, 2002, passim, und im Kontext mit vertrauenswürdigen Systemumgebungen *Landesbeauftragter für den Datenschutz Mecklenburg-Vorpommern (LfD)*, TCPA, Palladium und DRM, S. 6 f.; *Pfitzner* (o. Fußn. 5), S. 19 f. Der Text des *LfD* ist abrufbar unter: http://www.lfd.m-v.de/informat/tcpa/tcpa.pdf.

21) Ähnlich auch *Krogmann* u.a., BT-Drs. 15/660, S. 2. Vgl. des Weiteren *BITKOM* (o. Fußn. 1), S. 4.

22) Zu den urheberrechtlichen Aspekten vertrauenswürdiger Systemumgebungen vgl. etwa *Bundesregierung*, BT-Drs. 15/795, S. 6; *Koenig/O'Sullivan*, ECLR 2003, 449, 455 f.; *Stallman* (o. Fußn. 20), S. 115 f.

23) Zu den Vor- und Nachteilen aus Sicht des Datenschutzes vgl. *LfD* (o. Fußn. 20), S. 3 f.; *Dix/Pfitzner*, DuD 2003, 561; *Pfitzner* (o. Fußn. 5), S. 12 ff. S. des Weiteren die Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28.3.2003 in Dresden, TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden, S. 2 f.

24) S. hierzu oben, I. 1.

25) Nicht Gegenstand der Untersuchung sind auch weiterreichende wettbewerbsrechtliche Fragestellungen, die sich aus Aspekten vertrauenswürdiger Systemumgebungen ergeben, die über die Etablierung technischer Standards hinausgehen und etwa die Forschung und Entwicklung betreffen.

26) *Monopolkommission*, Wettbewerbspolitik oder Industriepolitik, Neuntes Hauptgutachten 1990/1991, BT-Drs. 12/3031, Tz. 811. Ausführlich *Gates*, Emory Law Journal 1998, Vol. 47 No. 2, 583, Sub III.

27) *Gleiss/Hirsch*, Komm. zum EG-Kartellrecht, Band 1, 4. Aufl. 1993, Rdnr. 330; *Immenga*, in: Immenga/Mestmäcker (Hrsg.), GWB, 3. Aufl. 2001, § 2 Abs. 1 Rdnr. 5. S. insoweit zu einem Mangel an Transparenz durch fehlende Standardisierung auf der Ebene des Kommunikationsinhalts *Neumann*, in: FS Celsen, 2001, S. 25.

28) *Gleiss/Hirsch* (o. Fußn. 27), Rdnr. 330; *Koenig/Kulenkampff/Kühling/Loetz/Smit*, Internetplattformen in der Unternehmenspraxis, 2002, S. 302; *Neumann*, in: Koenig/Bartosch/Braun (Hrsg.), EC Competition and Telecommunications Law, 2002, S. 617, 622; *Sucker*, CR 1988, 271.

29) *R. Bechtold*, GWB, 3. Aufl. 2002, § 2 Rdnr. 1; *Gates*, Emory Law Journal 1998, Vol. 47 No. 2, 583, Sub I.; *Schroeder*, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, Lbl., Stand: September 1999, Kap. 60 Rdnr. 13; *Shapiro*, Navigating the Patent Thicket: Cross Licenses, Patent Pools, and Standard-Setting, S. 21. Der Aufsatz von *Shapiro* ist abrufbar unter: http://faculty.haas.berkeley.edu/shapiro/thicket.pdf.

30) *Schroeder* (o. Fußn. 29), Kap. 60 Rdnr. 13.

31) *Gates*, Emory Law Journal 1998, Vol. 47 No. 2, 583, Sub III.; *Gawer/Cusumano*, Platform Leadership, 2002, S. 254; *Immenga* (o. Fußn. 27), § 2 Abs. 1 Rdnr. 6; *Monopolkommission* (o. Fußn. 26), Tz. 871.

32) *Immenga* (o. Fußn. 27), § 2 Abs. 1 Rdnr. 6; *Shapiro* (o. Fußn. 29), S. 21. Vgl. auch *Farrell/Saloner*, Rand Journal of Economics 1985, Vol. 16 No. 1, 70, 71; *Katz/Shapiro*, Journal of Economic Perspectives 1994, Vol. 8 No. 2, 93, 95 und 110; *Monopolkommission* (o. Fußn. 26), Tz. 881.

33) *Gey*, WuW 2001, 933, 934; *Koenig/Kulenkampff/Kühling/Loetz/Smit* (o. Fußn. 28), S. 301 und – einschränkend – S. 310 f. Ablehnend ggü. dem Konzept der Pfadabhängigkeit *Liebowitz/Margolis*, Regulation 1995, Vol. 18 No. 3, 33.

Betriebssysteme beherrschende Unternehmen *Microsoft*, für die Art. 82 EG maßgeblich ist (dazu unter 3.).

2. TCPA/TCG auf dem Prüfstand von Art. 81 EG

Standardisierungsvereinbarungen zwischen Unternehmen der gleichen Marktstufe verstoßen jedenfalls dann gegen das in Art. 81 Abs. 1 EG enthaltene Verbot der Wettbewerbsbeschränkung, wenn sie die Einhaltung der vereinbarten Standards rechtlich oder faktisch erzwingen sollen.[34] In diesen Fällen wird den beteiligten Unternehmen die Freiheit genommen, Produkte zu entwickeln und zu vertreiben, die mit dem vereinbarten Standard nicht übereinstimmen,[35] sodass der Wettbewerb unter ihnen insoweit beschränkt wird. Die *TCPA/TCG*-Spezifikationen sind aber weder für die Mitglieder noch für Dritte rechtlich oder faktisch verbindlich. Dies gilt selbst unter Anlegung geringster Anforderungen an die möglichen Folgen der Nichtbeachtung der Standards.[36]

Durch die Netzwerkeffekte, die in der Folge einer Standardisierung vertrauenswürdiger Rechnerplattformen zu erwarten sind,[37] können sich jedoch Marktzutrittsschranken für Dritte ergeben. Auch solche Beeinträchtigungen Dritter können aber einen Verstoß gegen Art. 81 Abs. 1 EG begründen, da die Gemeinschaftsorgane bei der Prüfung einer Wettbewerbsbeschränkung nicht nur auf die Handlungsfreiheit der Beteiligten, sondern allgemeiner auf die Konsequenzen für den Wettbewerb abstellen.[38] In diesem Zusammenhang spielen dann gerade die Auswirkungen auf (aktuelle und potenzielle) Wettbewerber, die nicht an der Vereinbarung beteiligt sind, eine zentrale Rolle.[39] Dieser weite Anwendungsbereich der Norm hat u.a. auch zur Folge, dass die Anwendung von Art. 81 Abs. 1 EG nicht auf horizontale Wettbewerbsverhältnisse beschränkt ist.[40] Erfasst werden somit auch Vereinbarungen, an denen Unternehmen unterschiedlicher Marktstufen beteiligt sind, wie dies bei der *TCPA/TCG* der Fall ist.

Eine potenzielle Beeinträchtigung der wettbewerblichen Möglichkeiten Dritter geht von der Standardsetzung durch ein Industriekonsortium insbesondere in zweierlei Hinsicht aus, wenn die Konformität mit dem betreffenden Standard zur faktischen Marktzutrittsbedingung wird. So erlangen zum einen die Mitglieder des Konsortiums Wettbewerbsvorteile gegenüber den Nichtmitgliedern, wenn die Mitglieder durch die Standardisierung einen Vorsprung an technischem Wissen erlangen, wenn Nichtmitglieder keinen Einfluss auf das Ergebnis der Standardisierung haben und wenn die Nichtmitglieder den Standard erst mit zeitlicher Verzögerung, insbesondere also erst nach seiner Veröffentlichung, übernehmen können.[41] Diese Voraussetzungen liegen bei Standardisierungsorganisationen regelmäßig vor und sind auch bei der *TCPA/TCG* gegeben.

Die Möglichkeiten Dritter, mit den Mitgliedsunternehmen in Wettbewerb zu treten, werden zum anderen aber auch dann beeinträchtigt, wenn zur Implementierung des Standards zwingend auf technische Verfahren zurückgegriffen werden muss, die durch gewerbliche Schutzrechte – namentlich Patente – geschützt sind.[42] Ein solcher Schutz betrifft zwar zunächst grundsätzlich außer dem Rechteinhaber selbst auch alle Mitglieder des Industriekonsortiums. Angesichts der Vielzahl der bei einer Standardisierung in Hochtechnologiebereichen regelmäßig berührten Schutzrechte ist es jedoch üblich, dass sich in diesen Bereichen tätige Standardisierungsorganisationen auf eine Politik im Bereich gewerblicher Schutzrechte (GSR)[43] einigen.[44] Diese begründet eine Verpflichtung der Mitglieder, sich bei der Implementierung des Standards möglicherweise erforderliche Lizenzen auf reziproker Basis zu vernünftigen und nicht diskriminierenden Bedingungen einzuräumen. Anders als die *TCPA* verfügt die *TCG* über eine solche GSR-Politik.[45] Nichtmitglieder haben jedoch keinen Anspruch auf eine Lizenzierung der zur Implementierung der *TCG*-Spezifikationen erforderlichen Schutzrechte, obwohl bei der Implementierung einer vertrauenswürdigen Rechnerplattform auf technische Verfahren zurückgegriffen werden muss, die durch *TCPA/TCG*-Mitglieder oder für diese patentiert wurden.[46]

Beide vorstehend genannten potenziellen Ursachen einer Wettbewerbsbeschränkung basieren auf der Unterscheidung zwischen Mitgliedern und Nichtmitgliedern. Gerade auch die Voraussetzungen für den Erwerb der Mitgliedschaft spielen daher für die Frage, ob die Standardisierungstätigkeit eines Industriekonsortiums eine Wettbewerbsbeschränkung darstellt, eine zentrale Rolle. Beschränkungen beim Erwerb der Mitgliedschaft können somit einen Verstoß gegen Art. 81 Abs. 1 EG zur Folge haben.[47] Die Statuten der *TCG* sehen verschiedene Kategorien der Mitgliedschaft vor: die „Adopters", die „Contribu-

---

34) Zu Grenzfällen einer faktischen Verpflichtungswirkung vgl. *Sucker*, CR 1988, 271, 272.

35) *Kommission*, Leitlinien zur Anwendbarkeit von Art. 81 EG-Vertrag auf Vereinbarungen über horizontale Zusammenarbeit, ABl. EG Nr. C 3 v. 6.1.2001, S. 2, Rdnr. 167. S. auch *Gleiss/Hirsch* (o. Fußn. 27), Rdnr. 328 und 331. Vereinbarungen, in denen eine unbedingte Festlegung auf einen Standard erfolgt, werden daher von der *Kommission* als wettbewerbsbeschränkend eingestuft, vgl. *Kommission*, Entscheidung 78/156/EWG (IV/29.151 – Video-Cassetterecorders), ABl. EG Nr. L 47 v. 18.2.1978, S. 42, Erwägungsgrund 23; *Sucker*, CR 1988, 271.

36) Ebenso für die entsprechende Frage der Standardisierung von Schnittstellen für B2B-Plattformen *Koenig/Kulenkampff/Kühling/Loetz/Smit* (o. Fußn. 28), S. 304 f.

37) Vgl. hierzu allg. die Ausführungen oben unter II. 1.

38) Zu dieser – auf keinem geschlossenen dogmatischen Konzept beruhenden – Praxis s. etwa *Koenig/Haratsch*, Europarecht, 4. Aufl. 2003, Rdnr. 819; *Roth*, CR 1988, 195, 196; *Roth/Ackermann*, in: Glassen/von Hahn/Kersten/Rieger (Hrsg.), Frankfurter Komm. zum Kartellrecht, Lbl., Stand: Dezember 2002, Art. 81 Abs. 1 EG-Vertrag Grundfragen Rdnr. 165.

39) *EuGH*, Rs. 32/65, Regierung der Italienischen Republik ./. Kommission der EWG, Slg. 1966, 457, 485; *Kommission*, Entscheidung 75/94/EWG (IV/23.013 – Goodyear Italiana – Euram), ABl. EG Nr. L 38 v. 12.2.1975, S. 10, Erwägungsgrund 6; *dies.*, Entscheidung 87/69/EWG (IV/31.458 – X/Open Group), ABl. EG Nr. L 35 v. 6.2.1987, S. 36, Erwägungsgrund 32; *Roth*, CR 1988, 195; *Weiß*, in: Calliess/Ruffert, Komm. zu EU-Vertrag und EG-Vertrag, 2. Aufl. 2002, Art. 81 EG Rdnr. 88 und 100 ff.

40) *EuGH* (o. Fußn. 39), S. 485; *R. Bechtold* (o. Fußn. 29), § 22 Rdnr. 25; *Koenig/Haratsch* (o. Fußn. 38), Rdnr. 816; *Roth/Ackermann* (o. Fußn. 38), Art. 81 Abs. 1 EG-Vertrag Grundfragen Rdnr. 165; *Schroeder* (o. Fußn. 29), Kap. 60 Rdnr. 4.

41) *Kommission*, Entscheidung 87/69/EWG (o. Fußn. 39), Erwägungsgrund 32; *Gleiss/Hirsch* (o. Fußn. 27), Rdnr. 329; *Roth*, CR 1988, 195; *Schroeder* (o. Fußn. 29), Kap. 60 Rdnr. 17; *Sucker*, CR 1988, 271, 272.

42) S. auch *Kommission*, XXV. Bericht über die Wettbewerbspolitik 1995, 1996, S. 140; *Shapiro* (o. Fußn. 29), Patent Thicket, S. 19.

43) Im angloamerikanischen Bereich wird eine solche GSR-Politik als „Reasonable And NonDiscriminatory (RAND) Policy" bezeichnet, vgl. hierzu auch *Haslach*, A Buyer's Guide to Special-Interests Groups, Sub „Reasonable and Nondiscriminatory License"; *Patterson*, Berkeley Technology Law Journal 2002, Vol. 17 No. 3, 1043, 1052 ff. Der Artikel von *Haslach* ist abrufbar unter: http://www.schwabe.com/showarticles.asp?Show=24.

44) *Shapiro*, Setting Compatibility Standards: Cooperation or Collusion?, S. 11. Zur GSR-Politik des *ANSI* (*Americans National Standards Institute*) vgl. *Stern*, IEEE Micro 1999, Heft 9/10, 7, 8. Zur GSR-Politik des *ETSI* (*European Telecommunications Standards Institute*) vgl. *Kommission* (o. Fußn. 42), S. 140 f.; *Neumann* (o. Fußn. 28), S. 683 f. Der Beitrag von *Shapiro* ist abrufbar unter: http://faculty.haas.berkeley.edu/shapiro/standards.pdf.

45) Section 16.4 der Bylaws of Trusted Computing Group, Stand: 26.2.2003.

46) Dies lässt sich bereits aus der Existenz der Sec. 16 der TCG Bylaws (o. Fußn. 45) folgern. S.a. den Hinweis zu Lizenzierungsanfragen bei *Pearson* (o. Fußn. 5), S. 281.

47) *Kommission*, Entscheidung 87/69/EWG (o. Fußn. 39), Erwägungsgrund 35; *Roth*, CR 1988, 195; *Schroeder*, in: Grabitz/Hilf (Hrsg.), Das Recht der Europäischen Union, Lbl., Stand: August 2002, Art. 81 EGV Rdnr. 594; *Sucker*, CR 1988, 271, 272. S.a. *Gates*, Emory Law Journal 1998, Vol. 47 No. 2, 583, Sub III.

tors" und die „Promoters".[48] Der Jahresbeitrag für Mitglieder in der untersten Kategorie der Mitgliedschaft, die „Adopters", beträgt 7.500 US-Dollar.[49] Für Unternehmen in Nischenbereichen stellt ein solcher regelmäßig zu entrichtender Mitgliedsbeitrag bereits eine nicht zu vernachlässigende Belastung dar. Diese wird für sich genommen zwar noch nicht zur Annahme einer Wettbewerbsbeschränkung führen können. Hinzu kommen aber drei weitere Aspekte:

- Zum Ersten sehen die *TCG*-Statuten erhebliche Beschränkungen der Mitwirkungs- und Informationsrechte der „Adopters" vor. Zur (zumindest weitgehend) gleichberechtigten Partizipation an den Wettbewerbsvorteilen, die sich aus der Beteiligung an der Standardisierungstätigkeit und dem dabei gewonnenen Wissen ergeben, muss ein Unternehmen faktisch der Mitgliedskategorie der „Contributors" angehören – zum doppelten Jahresbeitrag.[50]
- Zum Zweiten beschränkt sich die finanzielle Belastung eines Unternehmens, das Produkte auf Grundlage der *TCG*-Spezifikationen erstellen will, aber auch nicht auf den Mitgliedsbeitrag. Hinzu kommen vielmehr etwaige (angemessene) Lizenzgebühren. Diese dürften jedenfalls kurz- und mittelfristig weitgehend einseitig in Richtung der Gründungsunternehmen und der unmittelbar danach beigetretenen Mitglieder fließen.
- Und zum Dritten sehen die *TCG*-Statuten keine Abstufung der Beitragshöhe nach Jahresumsätzen oder anderen größenabhängigen Werten vor. Eine solche findet sich aber bei anderen Standardisierungsinitiativen wie dem *European Telecommunications Standards Institute (ETSI)* oder dem *W3-Konsortium*. Sie kann die Marktzutrittsschranken im wahrsten Sinne des Worts (abhängig von der Leistungsfähigkeit der Unternehmen) relativieren und somit für erhöhte Chancengleichheit im Wettbewerb sorgen. Nach alldem spricht somit viel dafür, dass hier (finanzielle) Marktzutrittshürden errichtet werden, die asymmetrisch zu Gunsten marktstärkerer Unternehmen wirken und eine Wettbewerbsverzerrung zu Lasten marktschwächerer Unternehmen bewirken.[51]

Ergänzend ist aus wettbewerbsrechtlicher Sicht noch kritisch darauf hinzuweisen, dass die wesentlichen Eckpunkte der Spezifikationen nicht etwa unter breiter Beteiligung der *TCPA*-Mitglieder zu Stande gekommen sind, sondern vor allem durch die Gründungsmitglieder gesetzt wurden. Gleiches gilt mit Blick auf den nächsten Evolutionsschritt der Spezifikationen, die noch für das Jahr 2003 erwartete Version 1.2, da diese wesentlich nicht mehr in der mittlerweile auf breiter Basis stehenden *TCPA*, sondern innerhalb der unter Beteiligung einer bislang lediglich kleinen Anzahl von Unternehmen neu gegründeten *TCG* erarbeitet wurde. Dieser zeitliche Aspekt korrespondiert mit entsprechenden wettbewerbsrelevanten Vorteilen beim Zugriff auf die neu standardisierten Technologien.[52]

Selbst wenn angesichts dieser beiden wettbewerbsrechtlichen Bedenken eine Wettbewerbsbeschränkung i.S.d. Art. 81 Abs. 1 EG vorliegen sollte, besteht aber noch die Möglichkeit einer Freistellung gem. Art. 81 Abs. 3 EG von dem dann grundsätzlich geltenden Verbot.[53] Im Kern wird dabei eine Abwägung zwischen den negativen Auswirkungen auf den Wettbewerb und den positiven Auswirkungen auf den technischen Fortschritt eingefordert, die von einer Standardisierung durch private Instanzen ausgehen. Durch Art. 1 Abs. 2 der Verordnung Nr. 1/2003,[54] die an die Stelle der bislang geltenden, aus dem Jahre 1962 stammenden Verordnung Nr. 17[55] tritt, wird ab dem 1.5.2004 insoweit ein Legalausnahmesystem gelten. In diesem sind die Wettbewerbsbehörden und Gerichte der Mitgliedstaaten nicht nur zur Anwendung der Art. 81 Abs. 1 EG und Art. 82 EG, sondern auch zur Anwendung von Art. 81 Abs. 3 EG und damit zu der insoweit erforderlichen wettbewerbspolitischen Abwägung befugt.[56] Dabei scheint im Falle der *TCG* eine Freistellung durchaus im Bereich des Möglichen, wenngleich angesichts der Unklarheiten über den tatsächlichen Nutzen vertrauenswürdiger Rechnerplattformen für die Verbraucher keinesfalls zwingend.

3. NGSCB auf dem Prüfstand von Art. 82 EG

Der Nexus einer künftigen „Windows"-Version wird Funktionen zur Verfügung stellen, die über eine bestimmte Softwareschnittstelle, das sog. Application Programming Interface (API), angesprochen werden. Dieses API müssen auch Drittanbieter berücksichtigen, wenn sie Programme für den Nexus entwickeln wollen. Insoweit wird also einseitig durch einen Marktteilnehmer ein technischer Standard etabliert. Anders als im Falle der *TCPA/TCG* bildet bei der Analyse der Entwicklung eines vertrauenswürdigen Betriebssystems auf Grundlage der NGSCB-Technologie daher nicht Art. 81 EG, sondern Art. 82 EG den wettbewerbsrechtlichen Bezugspunkt.[57] Insoweit soll von einer marktbeherrschenden Stellung des Unternehmens *Microsoft* auf

---

48) Sec. 1.1, 1.4 und 1.7 der TCG Bylaws (o. Fußn. 45). Vgl. auch die Übersicht unter http://www.trustedcomputinggroup.org/join/levels/.

49) *TCG* (o. Fußn. 12), Nr. 7.

50) Vgl. *TCG* (o. Fußn. 12), Nr. 7. Beim *ETSI* beträgt hingegen z.B. die Differenz zwischen dem Jahresbeitrag für einen ebenfalls nur mit eingeschränkten Rechten ausgestatteten „Observer" und dem Mindestjahresbeitrag für ein „Associate Member" unter € 2.000.

51) Die *TCG* hat auf die diesbezügliche Kritik mittlerweile reagiert und bereitet derzeit die Einführung neuer Mitgliedskategorien vor: Als „Advisor" sollen interessierte Dritte die Möglichkeit bekommen, die Standardisierungstätigkeit der *TCG* wissenschaftlich zu begleiten. Vor allem aber wird auch über die Ermöglichung einer kostenlosen Teilnahme an der Lizenzpolitik nachgedacht. Nur angedeutet werden sollen an dieser Stelle die Auswirkungen auf Entwickler sog. quelloffener, freier Programme, der sog. Open-Source-Software. Die meisten Open-Source-Entwickler dürften auf Grund der derzeitigen Mitgliedsbeiträge jedenfalls faktisch von der Mitgliedschaft in der *TCG* ausgeschlossen sein. Sofern auch bei der Entwicklung von Betriebssystemen und Applikationen, welche die Funktionalitäten der *TCPA/TCG*-Spezifikationen nutzen, auf geschützte Verfahren zurückgegriffen werden müsste, würde aber auch die Entwicklung spezifikationskonformer Programme faktisch behindert bzw. weitgehend ausgeschlossen.

52) Allgemein zur erhöhten Festlegungsmacht dominierender Unternehmen innerhalb von Standardisierungsorganisationen *Monopolkommission* (o. Fußn. 26), Tz. 871.

53) In der Vergangenheit sind bereits des Öfteren Vereinbarungen über Standards nach Art. 81 Abs. 3 EG freigestellt worden, vgl. etwa *Kommission*, Entscheidung 87/69/EWG (o. Fußn. 39), Erwägungsgründe 42 ff.; *dies.*, Fall 35207 – Sony (Minidiscs), 5.7.1995 (unveröffentl.), sowie dazu *Kommission* (o. Fußn. 42), S. 131.

54) Verordnung (EG) Nr. 1/2003 des Rates v. 16.12.2002 zur Durchführung der in den Art. 81 und 82 des Vertrags niedergelegten Wettbewerbsregeln, ABl. EG Nr. L 1 v. 4.1.2003, S. 1. Hierzu *Hossenfelder/Lutz*, WuW 2003, 118; *Koenig/Haratsch* (o. Fußn. 38), Rdnr. 825; *Montag/Rosenfeld*, ZWeR 2003, 107; *Weitbrecht*, EuZW 2003, 69.

55) Verordnung Nr. 17, ABl. EG Nr. P 13 v. 21.2.1962, S. 204, zuletzt geändert durch Verordnung (EG) Nr. 1216/1999 des Rates v. 10.6.1999, ABl. EG Nr. L 148 v. 15.6.1999, S. 5.

56) S.a. Erwägungsgrund 4 Verordnung Nr. 1/2003. Die Beweislast für das Vorliegen der Voraussetzungen der Freistellung vom Kartellverbot tragen dabei die Unternehmen, vgl. Art. 2 Verordnung Nr. 1/2003. Im Bereich der Standardisierung halten sich die praktischen Auswirkungen dieses grundsätzlichen Paradigmenwechsels freilich in engen Grenzen, da nach Art. 4 Abs. 2 Nr. 3 lit. a) der Verordnung Nr. 17 Vereinbarungen, Beschlüsse oder abgestimmte Verhaltensweisen, die lediglich die Entwicklung oder einheitliche Anwendung von Normen (Standards) zum Inhalt haben, schon bisher nicht anmeldepflichtig waren, vgl. auch *Koenig/Kulenkampff/Kühling/Loetz/Smit* (o. Fußn. 28), S. 308.

57) Zu dieser Schwerpunktverlagerung in einem anderen Zusammenhang auch *Koenig/Kulenkampff/Kühling/Loetz/Smit* (o. Fußn. 28), S. 309; *Köhler*, K&R 2000, 569, 579; *Sucker*, CR 1988, 271.

dem Markt für PC-Betriebssysteme ausgegangen werden.[58] Für die wettbewerbsrechtliche Beurteilung sind dabei drei Schwerpunkte auszumachen:

- Zum Ersten ist auf die vertikale Integration des Unternehmens *Microsoft* hinzuweisen, das gerade auch auf nachgelagerten Applikationsmärkten tätig ist. *Microsoft* ist daher mit komplementären Produkten Wettbewerber derjenigen Unternehmen, die auf den Zugang zum API angewiesen sind. Da *Microsoft* diesen Zugang kontrolliert, kann das Unternehmen somit Wettbewerbern den Marktzutritt erschweren, indem es den Zugang zum API beschränkt.[59] In einer solchen Beschränkung kann ein Marktmachtmissbrauch i.S.v. Art. 82 EG liegen.[60] Insoweit ist auf vergleichbare Konstellationen mit Blick auf andere „Windows"-APIs zu verweisen, die schon bislang einen zentralen Diskussionspunkt in der wettbewerbspolitischen Debatte um das Unternehmen *Microsoft* bilden.[61] Mit der Einführung des Nexus wird das wettbewerbsrechtliche Konfliktpotenzial insoweit quantitativ, aber nicht qualitativ erhöht.
- Zum Zweiten ermöglicht NGSCB vergleichbare Marktmachtverlagerungen aber auch in die entgegengesetzte Richtung. Als Gründungsmitglied sowohl der *TCPA* als auch der *TCG* kann *Microsoft* die Rahmenbedingungen von Märkten beeinflussen, die denjenigen Märkten, auf denen das Unternehmen tätig und marktstark ist, vorgelagert sind oder zu diesen sogar bislang noch nicht in jedem Fall einen spezifischen Bezug haben, also z.B. Märkte für Mobiltelefone, PDAs und Unterhaltungselektronik. Diese bereits durch die *TCPA/TCG* geschaffene Möglichkeit zur vertikalen Ausdehnung von Marktmacht wird durch NGSCB aber noch in erheblichem Maße verstärkt. Dies ergibt sich daraus, dass ein NGSCB-Betriebssystem hardwareseitige Anforderungen stellt, die über das hinausgehen, was in den *TCPA/TCG*-Spezifikationen festgelegt ist. Da die Unterstützung neuer technischer Möglichkeiten eines Betriebssystems des marktführenden Unternehmens einen faktischen Anpassungsdruck auf die betroffenen Hardwarehersteller ausübt, liegt hierin ein großes Vermachtungspotenzial auch hinsichtlich der Hardwareebene.[62]
- Zum Dritten eröffnet das Konzept vertrauenswürdiger Systemumgebungen *Microsoft* vor allem aber die Möglichkeit, die Interdependenzen zwischen der Betriebssystemebene über die sachnotwendig hiermit eng verbundene Ebene der Applikationen hinaus auf die Inhalteebene zu erstrecken. Indem ein vertrauenswürdiges Betriebssystem Inhalteanbietern zumindest bis zu einem bestimmten Grad die zentrale Kontrolle über die von ihnen übermittelten Informationen ermöglicht, können nämlich neue Möglichkeiten der Kooperation und Kollusion zwischen dem Hersteller des Betriebssystems und den zumeist ebenfalls marktmächtigen Inhalteanbietern geschaffen werden.[63] Zu denken ist hier insbesondere an DRM-Szenarien. Diese sind derzeit zwar allesamt noch spekulativer Natur. Da hier aber gerade die möglichen wettbewerbsrechtlichen Implikationen untersucht werden sollen, geht es gerade um diese Möglichkeit, i.R.e. vertrauenswürdigen Betriebssystems die Nutzung von Inhalten von der jeweiligen Systemumgebung abhängig zu machen.

Angesprochen sind damit Interdependenzen zwischen zwei getrennten sachlich relevanten Märkten, die es einem marktbeherrschenden Unternehmen erlauben, seine Marktmacht nicht nur auf dem beherrschten, sondern auch auf dem lediglich interdependenten Markt auszuüben. Unter besonderen Umständen[64] kann dabei ein Marktmachtmissbrauch i.S.d. Art. 82 EG auch dann vorliegen, wenn das betreffende Verhalten (nur) auf einem mit dem beherrschten Markt verbundenen Markt festgestellt wird und sich dort auswirkt.[65] NGSCB wird gegenseitige Abhängigkeiten und Einflussnahmemöglichkeiten schaffen, die in geradezu paradigmatischer Weise geeignet sein werden, solche besonderen Umstände zu begründen.

III. Fazit

Bei der Untersuchung der wettbewerbsrechtlichen Anforderungen an vertrauenswürdige Systemumgebungen ist zwischen den vertrauenswürdigen Rechnerplattformen, wie sie von der *TCPA/TCG* standardisiert werden, und der Entwicklung eines vertrauenswürdigen Betriebssystems durch das Unternehmen *Microsoft* zu unterscheiden. Im Kern geht es in beiden Fällen um wettbewerbsrechtliche Fragestellungen mit Blick auf die (gemeinschaftliche oder einseitige) Setzung technischer Standards. Diese sind freilich nicht erst mit „Trusted Computing" auf die wettbewerbsrechtliche Tagesordnung gekommen. Sowohl das Problem einer möglichen Wettbewerbsbeschränkung durch Standardisierungsinitiativen als auch die Gefahr eines Marktmachtmissbrauchs im Wege der Etablierung von Spezifikationen durch ein marktbeherrschendes Unternehmen haben sich insbesondere Ende der achtziger Jahre des vorigen Jahrhunderts erheblicher wettbewerbsrechtlicher Aufmerksamkeit erfreut. Und natürlich haben die verschiedenen kartellrechtlichen Verfahren, denen sich *Microsoft* in den letzten Jahren ausgesetzt sah, auch die Frage der Offenlegung von APIs umfasst.

Die eigentlich neue kartellrechtliche Dimension der Standardisierungsdebatte, welche durch das Konzept vertrauenswürdiger Systemumgebungen erreicht wird, liegt in der Schaffung neuer Interdependenzen mit bislang nicht hinreichend eng verbundenen Märkten, wobei es vorliegend insbesondere um Inhaltemärkte geht. Erst in den letzten zehn Jahren hat die Problematik interdependenter Märkte überhaupt nennenswerte wettbewerbsrechtliche Beachtung gefunden. Hier treffen neue technologische Möglichkeiten auf eine wettbewerbsrechtliche Dogmatik, die sich gerade erst im Entstehen befindet.

---

58) Vgl. auch *Kommission*, PM IP/01/1232; *U.S. District Court for the District of Columbia*, United States of America v. Microsoft Corporation, Findings of Fact v. 5.11.1999, Tz. 33 ff.; *Fleischer/Doege*, WuW 2000, 705, 711 f., m.w.Nw.

59) Zu möglichen Beschränkungsszenarien s. z.B. *Kommission*, PM IP/01/1232; *dies.*, Leitlinien für die Anwendung der EG-Wettbewerbsregeln im Telekommunikationsbereich, ABl. EG Nr. C 233 v. 6.9.1991 (nachfolgend: „TK-Leitlinien"), S. 2, Rdnr. 113; *Sucker*, CR 1988, 271, 274 f. *Microsoft* hat bereits angekündigt, das API offen zu legen, vgl. *Microsoft* (o. Fußn. 13), S. 3.

60) Vgl. *Jung*, in: Grabitz/Hilf (o. Fußn. 47), Art. 82 EGV Rdnr. 187 f. Mit Blick auf § 20 GWB: *Koenig/Kulenkampff/Kühling/Loetz/Smit* (o. Fußn. 28), S. 309.

61) S. etwa *Kommission*, PM IP/01/1232; *Fleischer/Doege*, WuW 2000, 705, 707; *Gawer/Cusumano* (o. Fußn. 31), S. 144. Vgl. des Weiteren *U.S. District Court for the District of Columbia* (o. Fußn. 58), Tz. 84 und Tz. 90 ff.

62) Schon in der Vergangenheit stand *Microsoft* im Verdacht, seine Marktmacht gerade auch ggü. *Intel* als wichtigstem, von der Unterstützung durch *Microsofts* „Windows"-Betriebssystem abhängigem Hersteller von Vorprodukten auszuüben, vgl. *U.S. District Court for the District of Columbia* (o. Fußn. 58), Tz. 103.

63) *Koenig/O'Sullivan*, ECLR 2003, 449, 453.

64) *EuGH*, Rs. C-333/94 P, Tetra Pak, Slg. 1996, S. I-5951, 6008, Rdnr. 27. Welche vom Einzelfall gelösten Umstände dies sein können, wurde vom *EuGH* bislang kaum näher konkretisiert, vgl. *Braun/Capito*, in: Koenig/Bartosch/Braun (o. Fußn. 28), S. 309, 342; *Koenig/Kühling/Braun*, CR 2001, 745, 749. S. GA *Colomer*, Schlussanträge zur Rs. C-333/94 P, Tetra Pak, Slg. 1996, S. I-5951, 5977, Nr. 57, der einige Kriterien entwickelt, welche der *EuGH* zumindest implizit aufgegriffen hat, vgl. *EuGH*, a.a.O., S. I-6008 f., Rdnr. 28.

65) *EuGH* (o. Fußn. 64), S. I-6008, Rdnr. 27. Vgl. auch *Jung* (o. Fußn. 60), Art. 82 EGV Rdnr. 123 m.w.Nw., sowie implizit *Kommission*, TK-Leitlinien (o. Fußn. 59), Rdnr. 113.