

„Trusted Computing“ – Kontrolliertes Vertrauen

Ausarbeitung im Rahmen der Vorlesung
Information Rules 1
TU Berlin

Clemens Brandt
Andreas Hinnerichs
Jörn Hoffmann

6. Januar 2004

Inhaltsverzeichnis

Vorwort	3
1 Einleitung	3
1.1 Die Idee hinter Trusted Computing	3
1.2 Technische Grundlagen	4
2 Spezifikationsgremien	5
2.1 Von der TCPA zur TCG	5
2.2 Aufbau der TCG	6
3 Auswirkungen auf die Computerbenutzung	6
4 Wirtschaftliche Folgen	8
4.1 Wirtschaft allgemein	8
4.2 IT Unternehmen	8
4.3 Innovationen und OpenSource	9
4.4 Europa und der Rest der Welt	10
5 Rechtliche Schranken	10
5.1 Amerika	10
5.2 Deutschland und Europa	11
6 Politische Aspekte	13
7 Fazit	14
A Literaturverzeichnis	16

Vorwort

Im Rahmen der Veranstaltung „Information Rules“ entwickelten wir diese Ausarbeitung zum Thema „Trusted Computing“ (TC). Ziel dieser Arbeit ist es, einen groben Überblick über dieses hoch aktuelle, jedoch zugleich sehr problematische Thema zu bieten. Problematisch in dem Sinne, da wir heute in einer Gesellschaft leben, in der wir uns von der Technologie immer abhängiger machen und andererseits Datenschutz und Integrität wahren wollen. Somit müssen Technologien geschaffen werden, die es einfach und doch effizient ermöglichen, Daten zu schützen und Personen zu identifizieren. Es ist ein Widerspruch schlechthin, der viele Fürsprecher und Gegner findet.

1 Einleitung

1.1 Die Idee hinter Trusted Computing

Das Volumen von Transaktionen im Internet wird auch in Zukunft weiterhin stark steigen [Gerstbach 2003]. Problematisch ist dabei jedoch, die schnellere Verbreitung von Viren und Trojanischen Pferden. Auch Cyber-Terrorismus, Online-Vandalismus, Diebstahl von Informationen und Identitäten werden mit Hilfe der weltweiten Vernetzung eher verstärkt. Trusted Computing will diesen Bedrohungen des Internetzeitalters entgegenwirken und sichere Geschäfte im Internet ermöglichen [Himmelein 2003].

Durch einen neuen plattformübergreifenden Sicherheitsstandard, der auf Hard- und Softwareebene zusammenarbeitet, soll dies erreicht werden. Für PCs, Notebooks, Server, PDAs und Handys wird er entwickelt, so dass frühzeitiges Erkennen von ungewollten Änderungen dann Viren, Hacker und Trojanische Pferde entlarven und stoppen soll. Weitere wichtige Punkte sind die Beglaubigung der Systemintegrität gegenüber Dritten, sowie die Sicherung der Anwenderdaten und kryptographischen Schlüssel vor Angriffen.

Geschaffen wird auch ein Fundament, welches grundlegende kryptographische Funktionen (Hash, Zufallsgenerator) bereitstellt, bestehende Sicherheitstechnologien (z.B. IPSec, VPN, S/MIME oder SSL) verstärkt und zusätzlich die Sicherheit der Hardware, beim BIOS und beim Betriebssystem erhöht. Der neue Schutz soll das

Vertrauen in E-Commerce und E-Business verbessern und bisher nicht da gewesene Möglichkeiten für Geschäfte im Internet erschließen [Gerstbach 2003].

1.2 Technische Grundlagen

Im folgenden Abschnitt soll nun geklärt werden, wie diese Ideen technisch realisiert werden können.

Grob gesehen besteht TC aus 4 Komponenten:

- Die Hardware (Trusted Platform Module (TPM) oder auch Fritzchip¹ genannt) schafft die Sicherheitsgrundlage mit Hilfe von Zertifikaten.
- Ein abgesicherter Speicher, der alle Sicherheitsrelevanten Daten (z.B. Status des Systems) speichert.
- Mehrere Sicherheitskernel im BIOS, Betriebssystem und den laufenden Applikationen
- Ein Netz öffentlicher Onlineserver, die von Hardware- und Softwareherstellern betrieben werden.

Die TPM überwacht ab dem Bootprozess die Plattform und mit Hilfe der Sicherheitskernel werden die Hard- und Software überprüft. Dadurch, dass jeder seinen Nächsten überprüft, wird eine „Kette des Vertrauens“ aufgebaut, die zuverlässig nicht gewollte Ereignisse erkennt [Gerstbach 2003]. Nun befindet sich das System in einem sicheren Zustand und es können TC-kompatible Software und Dokumente benutzt werden, da der Schlüssel vom Chip frei gegeben wurde [Anderson 2003a].

Vor und nach jeder durch TC gesicherten Online-Transaktion (z.B. E-Mail schreiben) wird mit Hilfe des Schlüssels der Status des Systems und die Identifikation verschlüsselt und ausgetauscht. Erst wenn beide Seiten zustimmen, wird die Transaktion korrekt ausgeführt. Bei jeder großen Änderung an der Konfiguration (z.B. neue Soundkarte usw.) muss man online seine Zertifikate erneuern.

¹ Benannt nach dem kalifornischen Senator Fritz Hollings, der einen Gesetzesentwurf, der TC-konforme Geräte vorschreibt, in Kalifornien durchsetzen wollte [McCullagh 2001].

TC bietet weiterhin die Möglichkeit, eine unbegrenzte Zahl von Geheimnissen vor Veränderung zu schützen. Jedoch wurde noch keine Funktion entwickelt, die diese Geheimnisse vor dem Löschen oder Benutzen schützt, da die Daten nicht innerhalb des TPMs abgelegt werden, sondern verschlüsselt auf einem externen Speicher liegen [Gerstbach 2003].

2 Spezifikationsgremien

2.1 Von der TCPA zur TCG

Die Trusted Computing Platform Alliance (TCPA) wurde am 11. Oktober 1999 durch die fünf Unternehmen Compaq, Hewlett-Packard, IBM, Intel und Microsoft gegründet.

Diese Industrievereinigung will das Vertrauen in Computerplattformen und deren Sicherheit bei Transaktionen im Internet erhöhen. So sollen mit ihrer Hilfe sicherheitstechnische Aspekte in Plattformen und Geräten besser integriert werden, d.h. zuerst Spezifikationen für sichere Technologien zu entwickeln und danach die Änderungen durch die Mitglieder durchzuführen und zu kontrollieren – sprich eine Zentralisierung der einzelnen Schritte [Gerstbach 2003].

Die TCPA ist eine basisdemokratische Vereinigung, wobei jedes Mitglied eine Stimme und Vetorecht hat. Demnach kommen Entscheidungen nur mit Zustimmung aller Mitglieder zustande. Jedes Unternehmen, das an der Entwicklung neuer Spezifikationen mitwirken möchte, wird von den Gründern eingeladen, der Allianz beizutreten. Diesem Aufruf folgten bis April 2003 über 200 Mitglieder [Himmelein 2003].

Am 8. April wurde eine Pressemitteilung der fünf Gründungsmitglieder der TCPA herausgegeben, in der die Gründung der Trusted Computing Group (TCG) bekannt gegeben wurde. Die TCG ist der offizielle Nachfolger von der TCPA. Die neue Gruppe von Unternehmen adaptiert und entwickelt alle bisherigen Spezifikationen weiter. Es wird vermutet, dass die Umbenennung mit der schwierigen Konsensfindung und der negativen Öffentlichkeitswirkung der TCPA zusammen hängt.

Da es bei über 200 Mitgliedern und nur einstimmigen Entscheidungen ein langwieriger Prozess war, neue Spezifikationen zu entwickeln, reicht nun bei der TCG eine Zweidrittelmehrheit [Gerstbach 2003].

2.2 Aufbau der TCG

Die Trusted Computing Group ist hierarchisch aufgebaut. Sie setzt sich zusammen aus einem Vorstand und verschiedenen Arbeitsgruppen und Sonderausschüssen, in welchen die Spezifikationen für die einzelnen Plattformen (PCs, Handys, PDAs) erarbeitet werden [TCG 2003b].

Es sind drei Arten von Mitgliedschaften möglich. An unterster Stelle stehen die „Adopters“. Sie müssen einen Jahresbeitrag von momentan 7500 \$ bezahlen und haben nur eingeschränkte Mitwirkungsrechte. „Adopters“ können nicht bei Arbeitsgruppen oder Sonderausschüssen mitarbeiten. Des Weiteren haben sie geringere Informationsrechte, was sich vor allem in der Website äußert, wo sie nur bedingt an Diskussionsgruppen und Mailinglisten teilhaben können.

An zweiter Stelle sind die „Contributers“ angesiedelt. Mitglieder dieser Art müssen 15.000 \$ pro Jahr bezahlen und können aktiv an der Erarbeitung der Spezifikationen teilnehmen. Des Weiteren können „Contributers“ im Gegensatz zu den „Promoters“ in den Vorstand gewählt werden.

Die einflussreichste Art der Mitgliedschaft bei der TCG ist die des „Promoters“. Mitglieder dieser Art müssen 50.000 \$ pro Jahr bezahlen, haben jedoch einen festen Platz in dem Vorstand der Organisation. „Promoter“ müssen mit einer Dreiviertelmehrheit gewählt werden.

Mitglied der TCG kann jedes Unternehmen werden, es existieren keine Aufnahmebedingungen. Der Vorstand hat jedoch das Recht, die Mitgliedschaft zu verwehren. Die TCG erstellt Spezifikationen, die offen zugänglich sind. Die Patente werden jedoch nur unter den Mitgliedern geteilt [Koenig 2003].

3 Auswirkungen auf die Computerbenutzung

Nach der aktuellen Spezifikation ist der „Trusted Mode“² Opt-In, also standardmäßig ausgeschaltet. Man kann demnach auch weiterhin nicht TC-konforme Software benutzen [TCG 2003c]. Wenn jedoch TC Software benutzt wird, so hat dies weitreichende Konsequenzen auf den Umgang und das Arbeiten am Computer.

² „Trusted Mode“ bedeutet, dass Trusted Computing aktiv ist.

Jedes Dokument, das man mit einer TC Software erstellt, wird verschlüsselt.

Entschlüsselt kann es dann natürlich auch wiederum nur mit TC Software werden. Die Folge liegt nahe: Sobald größere Gruppen, z.B. Unternehmen, auf TC umstellen, wird man indirekt dazu gezwungen es auch zu benutzen. Andernfalls ist die Entschlüsselung nicht möglich. Ein Aspekt dabei ist, dass durch die Verschlüsselung der Softwarehersteller festlegen kann, dass auch nur sein Programm verwendet wird, um Dateien zu lesen, die von seiner Software erstellt worden sind. Das heißt, wenn man zum Beispiel ein Word Dokument erhält, dass mit einem TC-Word erstellt wurde, benötigt man auch ein TC-Word, um es überhaupt lesen zu können [Anderson 2003b].

Softwarehersteller können durch die Verschlüsselung und dem Zertifizierungsmechanismus weiterhin sicherstellen, dass für Software immer bezahlt wird. Wenn ein Dokument von einem Programm verschlüsselt wurde, dessen Seriennummer auf einer „Blacklist“³ vorhanden ist, so kann der Empfänger dieses Dokumentes die Entschlüsselung verweigern [Anderson 2003b].

Ein anderer Aspekt bei der Verwendung von TC sind stärkere Zugangskontrollen für und von Dokumenten. Es ist möglich, Dateien personen- und zeitbezogen zu versenden. D.h. als Urheber kann man bestimmen wer wie lange ein Dokument zur Verfügung hat. Dies lässt bei E-Mails, vor allem aber bei Mediendateien wie MP3s interessante Möglichkeiten zu, die Nutzung und den Zugang zu Informationen zu kontrollieren [Anderson 2003a].

Als letzter Punkt muss noch auf die so genannten „Hintertüren“ eingegangen werden. Wie der Chaos Computer Club bereits mahnte [Hannich 2003], ist mit der derzeitigen Spezifikation ein entfernter Zugriff auf ein TC System möglich, ohne dass der Benutzer davon erfahren kann. Bei diesem Thema ist die Tür wilden Spekulationen leider weit geöffnet, weswegen wir nur gering darauf eingehen. Die Kontroverse besteht darin, dass zentrale Kontrollinstanzen, wie Zertifizierungsstellen, und sogar die Softwarehersteller selber, entfernt auf TC Computer zugreifen können. Zum Beispiel kann eine Software all meine MP3s löschen, die als illegal erachtet werden. Es ist sogar möglich, dass der Softwarehersteller selber meinen Computer durchsucht und darauf zugreift, ohne dass ich etwas davon mitbekomme, geschweige etwas dagegen unternehmen kann [Anderson 2003a].

³ Eine „Blacklist“ ist in diesem Zusammenhang eine Liste von Seriennummern von Programmen, die als illegal gehackt gelten.

An dieser Stelle kann man sich leicht verlaufen und sogar in Verschwörungstheorien geraten. Wir belassen es an diesem Punkt bei den Auswirkungen von TC auf den Benutzer.

4 Wirtschaftliche Folgen

4.1 Wirtschaft allgemein

Die Frage, die sich jedoch stellt ist, warum die TCG so weitreichende und umfassende Kontrolle auf den Benutzer erwirken möchte. Des Weiteren wird bei Betrachtung der Mitglieder schnell klar, dass es sich hauptsächlich um große Unternehmen handelt [TCG 2003a]. TC kann für sie ein Mittel sein, um Kunden enger an ihre Produkte zu binden.

Betrachten wir hierzu folgendes Beispiel: Derzeitig fallen bei dem Wechsel von Software für ein Unternehmen Kosten wie Installation, Umschulung und gegebenenfalls Dateikonvertierungen an. Die Kosten von einem Wechsel von zum Beispiel Microsoft Word zu Open Office sind bereits heute sehr hoch. Mit TC werden sie noch um einiges höher ausfallen. Sämtliche Word-Dateien, die von außerhalb bezogen werden, z.B. von Kunden oder Partnern des Unternehmens, sind nicht mehr lesbar. Das Unternehmen müsste von sämtlichen Urhebern die Erlaubnis in Form von digitalen Zertifikaten einholen – ein unvertretbarer Aufwand [Anderson 2003b].

Die Folgen sind klar, es werden nur wenige große Unternehmen davon profitieren. Neuen Produkten von kleineren IT-Firmen wird ein unsichtbarer Riegel vorgeschoben. Bereits heute gehen Unternehmen in ihrer Entscheidung für Software nach dem Kriterium der hohen Verbreitung. Mit TC besteht in gewissen Bereichen der Datenverarbeitung, wie zum Beispiel Textbearbeitung, ein Zwang für Unternehmen, sich für gewisse Produkte zu entscheiden.

4.2 IT Unternehmen

Neben der erwähnten Problematik der Marktkontrolle sind kleine und mittelständische Unternehmen mit TC noch in anderen Bereichen im Hintertreffen.

Nur wer Mitglied in der TCG ist, kann an der Spezifikation mitwirken (man muss jedoch mindestens den Status des „Contributors“ haben). Unternehmen mit einer geringen Finanzkraft können sich die Mitgliedschaft des „Contributors“ nicht leisten und sind damit ausgeschlossen. Zudem kommt noch, dass Unternehmen, die nicht in der TCG sind, in der Realisation der Spezifikation einen zeitlichen Rückstand haben. Weiterhin ist die Spezifikation zwar offen, die Patente teilen sich jedoch die TCG Mitglieder. Wie mit Außenstehenden umgegangen wird, ist noch nicht definiert worden [Koenig 2003].

Die Folgen davon sind eindeutig: TCG Mitglieder haben einen entscheidenden Marktvorteil. Die Mitgliedschaft ist mit Finanzkraft verbunden. Kleine und mittelständische Unternehmen sind somit im Nachteil gegenüber den großen Firmen.

4.3 Innovation und Open Source

Der Zweck von TC ist, dass Anwender vor fremden Zugriff und Manipulation geschützt werden sollen. Bestehende Dokumente und Anwendungen können nicht modifiziert werden [TCG 2003c].

Wenn man in die Geschichte der EDV zurückblickt, stellt man fest, dass viele nützliche Software dadurch entstanden ist, dass bestehende angefasst, erweitert und neu verknüpft wurde. Als Beispiel ist hier der Dateiserver SAMBA zu nennen. Er ist nur dadurch zu Stande gekommen, dass die Kommunikation von Client und Server abgehört wurde [Kühnel 1999].

An dieser Stelle ist auch der Einfluss von TC auf Open Source zu nennen. Natürlich ist TC auch mit Open Source Software möglich. IBM entwickelt bereits an einer Version von TC-Linux [Heise 2003]. Das Problem dabei ist jedoch, dass bei jeder Veröffentlichung von neuem Code dieser neu zertifiziert werden muss. Für den Open Source Entwickler bedeutet dies einen höheren finanziellen Aufwand, da die Zertifizierung natürlich nicht unendlich von statten gehen kann. Des Weiteren besteht auch ein höherer bürokratischer Aufwand. Dabei bleibt die Frage offen, ob ein Open Source Entwickler diese Hürden auf sich nehmen möchte. Der gesamte Open Source Prozess erhält einen erheblichen Schaden und ein weiterer Innovationsmotor wird blockiert [Anderson 2003b].

4.4 Europa und der Rest der Welt

Wie man anhand der Mitgliederliste erkennen kann, sind ein Großteil der Mitglieder der TCG amerikanische Firmen [TCG 2003a]. Es liegt nicht fern, dass jedes Unternehmen versucht, möglichst viele Vorteile aus TC für sich zu ziehen. Folglich liegen diese bei amerikanischen Firmen. Unter anderem kann sich dies darin äußern, dass die Kontroll- und Zertifizierungsinstanzen größtenteils in den USA liegen werden.

Ein wirtschaftlicher Schaden lässt sich aber auch anders für Europa herleiten. Europa ist stark in Open Source Technologien. Wie bereits erläutert, wird Open Source durch TC in seine Schranken getrieben. Zudem ist Europa stark im Smartcard Bereich. TC beinhaltet sämtliche Sicherheitsaspekte von Smartcards, was sie demnach überflüssig macht [Anderson 2003a]. Die Folge wird sein, dass Europa, vor allem im IT Sektor, noch mehr durch Amerika kontrolliert wird. Die Möglichkeiten für kleine und mittelständische Unternehmen, sich gegen die finanzkräftigen Unternehmen aus Übersee durchzusetzen, sind verschwindend gering.

5 Rechtliche Schranken

5.1 Amerika

Bei dem Vorhaben der TCG in dieser Größenordnung und den damit verbundenen weit reichenden Folgen stellt sich natürlich die Frage nach den rechtlichen Schranken. Blicken wir erst einmal auf die Vereinigten Staaten von Amerika. Im Mutterland von TC gibt es einen großen Vorantreiber in Sachen Trusted Computing, nämlich Senator Fritz Hollings, der dem Fritzchip seinen einprägsamen Namen gab. Senator Hollings legte 2001 einen Gesetzesentwurf vor, der TCG-konforme Geräte zur Pflicht für jedermann machen sollte [McCullagh 2001]. Die Strafe für den Verkauf oder auch nur Besitz von TC-freien Geräten sollte mit bis zu 5 Jahren Gefängnis und bis zu 500.000 \$ Geldstrafe geahndet werden. Nach Ansicht des anscheinend sehr sicherheitsbewussten Senators kann man den Terror nur bekämpfen, wenn man das Internet kontrolliert. Der Gesetzesentwurf scheiterte zwar, was Herrn Hollings aber nicht davon abhielt, einen zweiten Anlauf zu starten. So liegt nun wieder ein Entwurf für ein Gesetz vor, dessen Wege man aber nur schwer verfolgen kann. Bei der Suche nach dem momentanen Stand

bzw. Status des Gesetzes sind wir nicht fündig geworden, was die Annahme stärkt, dass es zwar (noch) nicht beschlossen, aber auch (noch) nicht abgelehnt wurde.

Auch wenn es abzusehen ist, dass Senator Fritz Hollings ein weiteres Mal scheitern wird, zeigt dieses Vorhaben doch, wie weit das Thema TC inzwischen von einer Überlegung einiger – zugegeben sehr mächtigen – Unternehmen die Leiter empor gestiegen ist und inzwischen ein wichtiger Kernpunkt betreffs der nationalen und internationalen Sicherheit ist. Gerade in Amerika, wo die Industrie die Regierung und die Gesetze stärker lenken kann, als es vielleicht nach unserem Verständnis gut wäre, geht man davon aus, dass die Gesetze, die der TCG im Weg stehen, eine Anpassung erfahren werden. Stichfeste Aussagen dazu gibt es zwar nicht, aber wer möchte angesichts der Disney-freundlichen Änderung des Urheberrechts⁴ ernsthaft daran zweifeln. Es gibt dann zwar kein Pflicht-TC, aber auch keine rechtliche Grundlage, die den Einsatz auf „freiwilliger“ Basis verhindert. Wie „freiwillig“ jedoch solch ein Einsatz sein wird, ist bei den Namen der beteiligten Unternehmen (Microsoft, Intel, AMD, HP, um nur einige zu nennen) sehr fraglich.

5.2 Deutschland und Europa

Da sich durch die EU das deutsche und das europäische Recht in den grundsätzlichen Aussagen sehr ähneln – zumindest in dem hier fokussierten Bereich – betrachten wir nur Deutschland. Einen Einfluss der Industrie, wie in Amerika, gibt es in dieser Größenordnung in Deutschland nicht. Selbst wenn, würde sie in Sachen TC sicher nicht eine pro-TCG Haltung einnehmen. Eine Bereinigung der hiesigen Gesetze wird es also vermutlich nicht geben, was uns die Betrachtung einfacher macht.

Auf der Suche nach einer Kollision mit einem gültigen Gesetz stößt man ziemlich schnell auf das Datenschutzgesetz. Mit „Daten“ sind hier nicht die Daten auf dem Computer gemeint, die der Benutzer vielleicht vor hat, zu verschlüsseln, sondern die personenbezogenen Daten, die raus in die weite Welt geschickt werden sollen, um mich und meinen Computer auch wirklich als mich und meinen Computer zu identifizieren. Diese Identifikation nehmen die Zertifizierungsstellen vor, die aller Voraussicht nach zumindest zum größten Teil in Amerika ihren Sitz haben werden. Es kommt also zu einem – vom Benutzer kaum beeinflussbaren – Datenfluss von Deutschland nach

⁴ Die Copyright-Frist für künstlerische Werke bei Einzelpersonen nach dem Ableben des Urhebers wurde auf 95 Jahre verlängert [CTEA 1998]. Das Urheberrecht des Disney-Konzerns an der frühesten Version der Figur Micky Maus ("Steamboat Willie") wäre sonst in diesem Jahr ausgelaufen.

Amerika. Gerade das ist aber nach den EU-Richtlinien bzgl. des Datenschutzes nicht erlaubt, da eine Datenübermittlung nur noch in Länder erfolgen darf, die mit dem EU-Recht vergleichbare Datenschutzbedingungen anbieten. Dazu gehören z. B. die Schweiz, Ungarn, Norwegen und auch Kanada, nicht aber die Vereinigten Staaten von Amerika [Heidrich 2003].

Können wir uns jetzt also zurücklehnen und uns „sicher“ fühlen, geschützt durch unsere Gesetze? Nein, denn ein Gesetz hat den Nachteil, darauf zu warten, dass es auch einer benutzt. Und im Falle des Datenschutzgesetzes wartet es zum Teil noch heute darauf. Der Internetversandhändler Amazon.de (Deutschland) sendet z. B. fleißig personenbezogene Daten seiner Kunden an Amazon.com (Amerika), ebenso verfahren Ebay und andere Unternehmen mit Niederlassungen in Deutschland und Hauptsitz in Amerika. Woran liegt das? Die Zeitschrift iX hat sich in einem Artikel diesem Thema gewidmet und bei Amazon wie auch bei der zuständigen Datenschutzbehörde nachgefragt. Das Ergebnis war nicht überraschend. Amazon beruft sich darauf, noch keinerlei Beschwerden von Kunden wegen ihres Verstoßes gegen die Datenschutzgesetze erhalten zu haben und die zuständige Behörde gibt unverständliche Erklärungen ab, weshalb alles doch seine Ordnung hat [Heidrich 2003].

Es wird eines deutlich: ein Gesetz wird erst dann Anwendung finden, wenn der Geschädigte es auch anwenden will – vorausgesetzt er weiß überhaupt, dass ein solches Gesetz existiert. Der Geschädigte bei Amazon ist der Kunde, der aber die Vorteile dieses Versandhändlers nutzen möchte und daher auch ein paar Gesetzesübertretungen toleriert. Der Geschädigte bei TC ist der Besitzer bzw. der Benutzer des Computers, der aber sicherlich auch weiterhin einen Prozessor von Intel oder AMD sein Eigen nennen möchte und sich an sein Microsoft Windows und Office gewöhnt hat. Wie viel Chancen hat das Gesetz also hier, seine Anwendung zu finden? Wie viel Marktmacht benötigt ein Unternehmen, um ein Gesetz geschickt zu umgehen? Die Fragen sind wahrlich nicht pauschal zu beantworten, doch wenn man sich die Namen der Mitglieder der TCG noch einmal vor Augen führt, wird deutlich, dass eine Ablehnung von TC nicht auf Benutzerebene funktioniert, sondern viel höher angegangen werden muss.

6 Politische Aspekte

Im März 2003 auf der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder gab es eine Entschließung mit Titel „TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden“. Die Kernaussage dieser Entschließung findet man am Ende des Dokuments: „Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb Hersteller [...] auf, [...] dass Anwenderinnen und Anwender die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik haben [...].“ [BfD 2003] In diesem Satz wird das Ausmaß von TC deutlich. Der Anwender hat nicht mehr die Kontrolle über die genutzte Informationstechnik, er hat keine Kontrolle mehr über seinen Computer. Was für den normalen Anwender ein großes Übel ist, ist in diesem Fall für Regierungen eine Katastrophe. Kein Industrieland dieser Welt kann inzwischen ohne Informationstechnik regiert werden. Computer arbeiten unbemerkt im Hintergrund und regeln unseren täglichen Ablauf. Kontrolliert werden diese Computer von der von uns gewählten Regierung, die damit unser Vertrauen genießt. Bis jetzt ist das so. Mit TC wird die Kontrolle aber in andere Hände gelegt – in die Hände der Hersteller und der Zertifizierungsstellen, also hauptsächlich nach Amerika. Amerikanische Unternehmen kontrollieren dann nicht nur meinen Computer zu Hause, sondern auch die Computer des Innenministeriums. Bei der engen Zusammenarbeit und dem großen Entgegenkommen amerikanischer Regierungen und der Industrie kann man diese Aussage getrost erweitern und behaupten, dass die amerikanische Regierung die Computer nicht nur unserer Regierung, sondern aller Regierungen kontrolliert, die auf TC basierte Informationstechniken nutzen.

Auf einem TCG Symposium in Berlin formulierte Ross Anderson es so: „Im Jahre 2010 wird Präsidentin Hillary Clinton zwei rote Knöpfe auf ihrem Schreibtisch haben: einer, der die Raketen Richtung China abfeuert und einer, der sämtliche chinesischen PCs abschaltet. Und nun raten Sie mal, welchen Knopf die Chinesen am meisten fürchten.“ [Anderson 2003a]. Der Zwischenruf aus dem Publikum, was denn mit dem Knopf für Europa sei, ist nur die logische Weiterleitung dieser Horrorvision, die nach den Wünschen der TCG jedoch schon bald zur Realität werden könnte. Wir möchten hier den Herstellern keine Absicht oder gar gezieltes Vorhaben unterstellen, die Informationstechnik anderer Länder kontrollieren zu wollen, aber allein das Vorhandensein solcher Möglichkeit müsste den Verantwortlichen für innere und äußere Sicherheit große Sorgen bereiten.

Die Kontrolle über einen Computer zu haben ist eine Sache, doch es gibt eine vielleicht noch schwerwiegendere Lücke im TCG-Universum. Für den Identifikationsvorgang werden wie schon erwähnt Daten gesendet – Daten, die eigentlich nur und ausschließlich zum korrekten Identifizieren notwendig sind. Welche Sicherheit gibt es aber dafür, dass nicht umfangreichere Datensammlungen verschickt werden? Keine, denn die zu versendenden Daten werden mit 2048 Bit verschlüsselt und sind daher für fremde bzw. in diesem Fall eigene Augen nicht zu erkennen. Die jetzige Spezifikation, die ausdrücklich Hintertüren ermöglicht, trägt da nicht gerade zur Beruhigung bei. Was ist also, wenn Daten für die außenpolitische Sicherheit eines Landes auf einmal auf dem Schreibtisch des Präsidenten eines anderen Landes liegen? Unvorstellbar? Nicht mit Trusted Computing und der TCG. Was diese Abhängigkeiten und Kontrollmöglichkeiten bei einem Krisenfall für Auswirkungen hätten, mag man sich gar nicht vorstellen.

7 Fazit

Trusted Computing in der jetzigen Form der TCG ist nicht nur ein Vorhaben mit äußerst negativen Folgen, sondern vor allem eines: gefährlich. Nicht unbedingt gefährlich für den einzelnen Benutzer, schon leicht gefährlich für mittelständische Unternehmen, aber vor allem sehr gefährlich für die Souveränität der einzelnen Länder. Nach der Einführung und Verbreitung von TC gäbe es eigentlich nur noch zwei Sorten von souveränen Staaten, nämlich die Länder, die keine Informationstechnologien einsetzen und die Vereinigten Staaten von Amerika. Um das zu verhindern, muss Europa, als momentan einziger großer Gegenpol zu den Vereinigten Staaten, gegenhalten und endlich Willen, Stärke und Einheitlichkeit demonstrieren.

Eine mögliche Folge wäre die Umgestaltung der TCG zu einer öffentlichen Zusammensetzung, die aus verschiedenen Parteien unterschiedlicher Bereiche und Schichten besteht. Nach dem Vorbild des W3Cs⁵ könnte man so neue Standards entwickeln, die einer weltweiten Überprüfung standhalten müssten bevor sie eingesetzt werden. Allein durch die Willkür weniger Unternehmen nur eines Landes ist der ernsthafte Einsatz von TC momentan inakzeptabel.

⁵ <http://www.w3.org> [6 Januar 2004]

Auch ein verstärktes Einsetzen von Open Source Lösungen würde das Vorhaben der TCG erschweren, wenn nicht sogar völlig unmöglich machen. Solange wir und vor allem die Regierungen aber weiter an Microsoft und Windows festhalten, wird es ein Leichtes sein, völlig schleichend und für viele unbemerkt, TC auf die Computer zu bringen. Der Einsatz von Open Source würde aber zeigen, dass man sich nicht von den Herstellern den Weg vorschreiben lässt, sondern den eigenen Weg geht – auch wenn er im ersten Moment vielleicht noch etwas holprig ist. Nur so bewahrt man sich seine Souveränität.

Das eigentliche Problem ist aber viel subtiler. Es herrscht einfach Unwissenheit und Unklarheit überall. Wie kann ich etwas verhindern, von dem ich nicht mal weiß, dass es existiert? Und warum sollte ich es verhindern, wenn mir die Hersteller doch so viel mehr Sicherheit dadurch versprechen? Hier hat die TCG durch ständige Namensänderungen gute Arbeit geleistet. Es herrscht mehr Verwirrung als Klarheit und kaum einer kann den völligen Umfang wirklich begreifen. Auch wenn sich dieses Thema vorrangig um Recht und Politik dreht, darf die Auseinandersetzung damit nicht bei den Juristen bleiben. Es muss die Aufgabe der Informatiker sein, Licht ins Dunkel zu bringen und die wirklichen Gefahren aufzudecken. Erst wenn die Gesellschaft und damit auch die Politiker für dieses Thema sensibilisiert wurden, kann man sie auch mobilisieren. Und erst dann haben wir die Sicherheit, dass die Zukunftsvision von Ross Anderson nicht zur Realität wird, sondern Utopie bleibt.

A Literaturverzeichnis

Anderson 2003a ANDERSON, Ross: *'Trusted Computing' Frequently Asked Questions - TC / TCG / LaGrande / NGSCB / Longhorn / Palladium / TCPA*. Cambridge University. August 2003. - online:

<http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html> [25 November 2003]

Anderson 2003b ANDERSON, Ross: *Cryptography and Competition Policy – Issues with ,Trusted Computing‘*. Cambridge University. 2003.– online:

<http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tcpa.pdf> [25 November 2003]

BfD 2003 BfD: *65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Der Bundesbeauftragte für den Datenschutz*, März 2003. – online:

http://www.bfd.bund.de/information/DS-Konferenzen/65dsk_ent2.html
[06 Januar 2004]

Gerstbach 2003 GERSTBACH, Peter; TOMEK, Andreas: *Trusted Computing*. Universität Wien 2003 – online: http://www.uniprojekt.org/tc/trusted_computig.pdf
[25 November 2003]

CTEA 1998 CTEA: *Copyright Term Extension Act*, Senate and House of Representatives, Oktober 1998. – online:

<http://www.techlawjournal.com/courts/eldritch/pl1105-298.htm> [06 Januar 2004]

Hannich 2003 HANNICH, Matthias: *Kontrolliertes Vertrauen*. In: *Telepolis* (2003). – Telepolis, 28 August 2003, online:

<http://www.heise.de/tp/deutsch/inhalt/te/15451/1.html> [25 November 2003]

Heidrich 2003: HEIDRICH, Joerg: *Datenwanderung*. In: *iX* (2003), Nr. 5, S. 96. – online:

<http://www.heise.de/ix/artikel/2003/05/096/> [06 Januar 2004]

Heise 2003: HEISE: *Linux-Treiber für TCPA Version 1.1b von IBM verfügbar*.

In: *heise newsticker* (2003). – heise newsticker, 15 August 2003, online:

<http://www.heise.de/newsticker/data/rh-15.08.03-000/default.shtml>
[25 November 2003]

Himmelein 2003 HIMMELEIN, Gerald: *Trusted Computing – Ein kurzer Spaziergang*.

In: *heise c't-online* (2003). – Linux-Tag 2003, Juli 2003, online:

<http://www.heise.de/ct/Redaktion/ghi/tc/linuxtagTC.html>
[25 November 2003]

Koenig 2003 KOENIG, Christian: *Workshop Sektion 5: Marktzugangsprobleme, vor allem für die Mittelständische Softwarebranche*. Symposium "Trusted Computing Group" (TCG) des Bundesministeriums für Wirtschaft und Arbeit (BMWA) in Berlin. – online:

<http://www.tkrecht.de/vortraege/bmwa2003/tc-workshop-rede20030703.pdf>
[25 November 2003]

Kühnel 1999 KÜHNEL, Jens: *SAMBA - Wanderer zwischen den Welten*. Linux-Tag 1999. – online:

http://www.unix-ag.uni-kl.de/~linux/linuxtag99/samba_wanderer_zwischen_den_welten.html [25 November 2003]

McCullagh 2001 MCCULLAGH, Declan: *Security Systems Standards and Certification Act*. September 2001. – online:

<http://www.politechbot.com/docs/hollings.090701.html> [06 Januar 2004]

TCG 2003a TCG: *List Of Current Members*. November 2003. – online:

<https://www.trustedcomputinggroup.org/about/members/> [25 November 2003]

TCG 2003b TCG: *Bylaws of Trusted Computing Group*. 20 March 2003. – online:

https://www.trustedcomputinggroup.org/about/tcg_bylaws.pdf
[25 November 2003]

TCG 2003c TCG: *Backgrounder*. May 2003. – online:

https://www.trustedcomputinggroup.org/downloads/TCG_Backgrounder.pdf
[25 November 2003]