Deutscher Bundestag **Drucksache 15/795**

15. Wahlperiode 07. 04. 2003

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Martina Krogmann, Günter Nooke, Bernd Neumann (Bremen), weiterer Abgeordneter und der Fraktion der CDU/CSU – Drucksache 15/660 –

Auswirkungen des „Trusted Platform Module“ und der Software „Palladium“

Vorbemerkung der Fragesteller

International führende Unternehmen der Computerindustrie haben sich zu der Trusted Computing Platform Alliance (TCPA) mit dem Ziel zusammengeschlossen, einen Standard für eine Hardware-Sicherheitsplattform für Personal Computer zu entwickeln. Dabei soll ein Hardware-Sicherheitsmodul, das so genannte TPM („Trusted Platform Module“) in die Rechner, später eventuell in die Prozessoren, integriert werden.

Das TPM kann verwendet werden, um den Benutzer zu identifizieren, Verschlüsselungen zu erzeugen sowie Zertifikate zu verifizieren und zu nutzen etc. Zusätzlich kann es durch Überwachung des Bootvorgangs auf Anfrage einen vertrauenswürdigen Zustand des Rechners attestieren und Manipulationen an der Rechnerkonfiguration oder am Betriebssystem ausschließen. Es überprüft bei jedem Start des Computers alle Hardware-Komponenten und das BIOS, dann das Betriebssystem sowie bestimmte Anwendungen auf die Übereinstimmung mit den von der TCPA zertifizierten und – anwendungsabhängig – auf externen Servern hinterlegten Konfigurationsangaben. Dadurch kann das TPM die Integrität der installierten Hard- und Software erkennen und kontrollieren, ob Programme, Software, Dokumente, etc. in einer für Inhaber von Rechten an Programmen und Daten akzeptablen Form genutzt werden.

Während bereits die ersten Computer mit einem TPM ausgerüstet sind, ist derzeit noch nicht konkret absehbar, wann die Firma Microsoft das Schutzssystem „Palladium“, eine Betriebssystem-Schnittstelle für die von der Hardware vorbereitete sichere Umgebung, einführen wird. „Palladium“ (neuerdings: NGSCB, Next Generation Secure Computing Base) soll ein integrierter Bestandteil zukünftiger Betriebssysteme der Firma Microsoft werden und kann auf die vom TPM bereitgestellten Funktionen aufsetzen. „Palladium“ erlaubt den Betrieb aller bisheriger Windows Software, aber über TCPA-Hardware auch neue, speziell für TCPA/Palladium geschriebene Applikationen und Datenformate.

Von der neuen Technologie erhoffen sich Anbieter urheberrechtlich geschützter digitaler Inhalte eine deutliche Verbesserung der Durchsetzbarkeit ihrer Nutzungs- und Verwertungsrechte, zum Beispiel auch gegen illegale Nutzung

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 3. April 2003 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

und Verbreitung geschützter Inhalte. Denkbare Anwendungsszenarien sind ferner der bessere Schutz von Firmennetzwerken, die Eindämmung von Attacken, die Sicherung von E-Government-Anwendungen oder der Schutz vor Schadprogrammen.

Andererseits werden durch die neue Technologie neue Nutzungs-, Partizipations- und Rechtsverhältnisse geschaffen. Erstmals können bestimmte Verhaltensweisen erzwungen werden, damit der Rechner für den Nutzer wichtige Inhalte verarbeitet. Die Intransparenz TPM-basierter Software und neue Lizenzierungsmodelle für Programme und Inhalte könnten negative Folgen für den Wettbewerb in der Hard- und Software-Branche, die gerade in Deutschland durch kleine und mittlere Unternehmen geprägt ist, nach sich ziehen. Der Nutzer könnte mit TCPA und „Palladium“ effektiv in seinen Rechten eingeschränkt und in seiner Privatsphäre verletzt werden. Es ist nicht mehr kontrollierbar, ob verschlüsselte Software schädliche Zusatzfunktionen enthält, z. B. so genannte „Spyware“ oder fernsteuerbare Funktionen. Durch die kryptografischen Funktionen der sicheren Hardware abgesichert, könnten auch kriminelle und terroristische Netzwerke sicherer kommunizieren. Damit ergeben sich neue Probleme im Zusammenhang mit Datenschutz, Schutz vor Industriespionage sowie für Aspekte der inneren Sicherheit.

Der Kenntnisstand in der deutschen Öffentlichkeit über TCPA und „Palladium“ ist bisher äußerst gering. Die zahlreichen, heute nur schwer absehbaren Auswirkungen werden kontrovers und mit Sorge diskutiert.

1. Welche Maßnahmen trifft das Bundesamt für Sicherheit in der Informationstechnik (BSI) bezüglich TPM/Palladium?

Im BSI wurde eine Projektgruppe zum Thema TPM und Palladium (zwischenzeitlich in NGSCB – Next Generation Secure Computing Base – umbenannt) eingerichtet, die die verifizierbaren Informationen sammelt und bewertet sowie erste mit TPM ausgestattete Systeme prüft.

2. Wann und zu welchem Zweck wurde eine entsprechende Arbeitsgruppe am BSI gegründet?

Die Projektgruppe wurde am 1. August 2002 eingerichtet mit dem Ziel, die Entwicklungen und Folgerungen aus „TPM/Palladium“ zu beobachten und kritisch zu prüfen.

3. Wie viele Mitarbeiter umfasst diese Arbeitsgruppe?

Die Projektgruppe umfasst insgesamt 17 Mitarbeiter.

4. Welche Erkenntnisse liegen der Arbeitsgruppe bisher vor?

Die Firmen Compaq/Hewlett-Packard, IBM, Intel und Microsoft waren die Gründungsmitglieder der „TCPA (Trusted Computing Platform Alliance)“, die eine hardware-basierte Lösung zur Bewältigung von IT-Sicherheitsprobleme anstrebten. Die TCPA umfasst mittlerweile rund 200 Firmen weltweit. Die TCPA hat auch eine Spezifikation eines Sicherheits-Chips (TPM-Chip, „Trusted Platform Module Chip“) festgelegt, von dem es bereits realisierte Versionen gibt. Von der Firma IBM sind bereits Notebooks mit diesem Chip auf dem Markt. Diese Realisierung dient jedoch hauptsächlich dem hardwaremäßigen Schutz der Geräte und unterscheidet sich damit grundlegend – auch in der Rechte- und Schlüsselverwaltung – von dem „Palladium“-Konzept, das wesentlich mehr Veränderungen in der Hardware bedingen würde.

Zum gegenwärtigen Stand von „Palladium“ ist zu sagen, dass von der Firma Microsoft bisher nur verschiedene Konzepte vorliegen, aus denen sich noch keine eindeutige Realisierung ableiten lässt. Insbesondere ist noch nicht festgelegt, welche spezifischen Berechtigungen der Administrator und auch der einzelne Benutzer erhält. Außerdem ist noch offen, wie die diversen Registrierungen und Überprüfungen der verschiedenen Schlüssel, die zur Absicherung benötigt werden, vorgenommen werden und wo sie zur Überprüfung gespeichert werden.

Erst wenn die Realisierung von „Palladium“ und des zugehörigen TPM einen Status erreicht haben, bei dem tatsächlich Aussagen hinsichtlich der Auswirkungen auf den Benutzer von „Palladium“-Rechnern möglich sind, kann die Arbeitsgruppe des BSI diese auch treffen.

5. Beabsichtigt die Bundesregierung entsprechende Erkenntnisse des BSI regelmäßig zu veröffentlichen?

   Wenn ja, in welchem Zeitraum?

   Wenn nein, warum nicht?

Sobald die Erkenntnisse zu TPM und Palladium so belastbar und verdichtet sind, dass eine Bewertung möglich ist, wird die Bundesregierung sie in geeigneter Form veröffentlichen.

6. Inwieweit ist der Bundesbeauftragte für den Datenschutz bereits mit der TCPA/Palladium-Problematik befasst und was ist seine Einschätzung?

Der Bundesbeauftragte für den Datenschutz ist bereits seit längerem mit den Themen TCPA und Palladium befasst. Er befürwortet alle Aktivitäten, die auch in diesem Zusammenhang der Verbesserung des Datenschutzes dienen und insbesondere zu einer manipulations- und missbrauchssicheren sowie transparenten IT-Infrastruktur führen. Auf der anderen Seite hat er Verständnis für die berechtigten Forderungen der Softwarehersteller, dass kostenpflichtige Software nur bei Bezahlung genutzt werden darf.

7. Beabsichtigt die Bundesregierung, die Auswirkungen dieser neuen Technologie in Anbetracht ihrer Bedeutung auf europäischer Ebene zu thematisieren?

   Welche Gremien wären hier nach Meinung der Bundesregierung zuständig?

Die Bundesregierung beabsichtigt angesichts der Erkenntnislage (s. Antwort zu Frage 4) derzeit nicht, die Auswirkungen der neuen Technologie TCPA/Palladium auf europäischer Ebene zu thematisieren.

8. Welche wirtschaftlichen Chancen/Risiken sieht die Bundesregierung durch TCPA für die digitale Wirtschaft?

Die Bundesregierung geht davon aus, dass das TCPA-Projekt mittelfristig Auswirkungen auf bestimmte Wirtschaftsbranchen haben wird; so vor allem auf die Smartcardhersteller, auf die IT-Sicherheitsbranche sowie auf einzelne Softwareentwicklerfirmen. Noch unklar ist allerdings, unter welchen Voraussetzungen und in welchem Umfang es hier auch zu Beeinträchtigungen kommen

kann. Das Bundesministerium für Wirtschaft und Arbeit (BMWA) beabsichtigt deshalb, im Frühsommer 2003 ein Symposium zu veranstalten, auf dem u. a. die Frage nach den Auswirkungen von TCPA/Palladium auf die deutsche Wirtschaft umfassend behandelt werden soll. Im Rahmen dieses Symposiums sollen auch Vertreter der betroffenen Wirtschaftsbranchen sowie von TCPA und Palladium Gehör finden.

9. Welche Chancen/Risiken sieht die Bundesregierung in der Realisierung eines hardwaregestützten sicheren Betriebssystems?

Die Chance eines hardware-gestützten Betriebssystems liegt darin, dass Programme mit Schadensfunktion (Computer-Viren, Trojanische Pferde, etc.) nicht in der Lage sind, dass Betriebssystem zu verändern. Die Risiken liegen darin, dass Fehler im Betriebssystem nicht mehr einfach beseitigt werden können. Bei der Implementierung muss zudem sichergestellt sein, dass ein hardware-gestütztes Betriebssystem nicht zu große Einschränkungen bei der Nutzung von Rechnern zur Folge hat. Nach ersten Informationen bietet der technische Ansatz von „Palladium“ grundsätzlich Möglichkeiten zum umfassenden Schutz sensitiver Daten vor unberechtigtem Zugriff.

10. Wie beurteilt die Bundesregierung in der Öffentlichkeit wiederholt geäußerte Befürchtungen einer möglichen restriktiven Lizenzierungspolitik für die Hard- und Software?

Aufgrund der bisher bekannt gewordenen technischen Konzeption kann noch nicht abschließend beurteilt werden, welche konkrete Lizensierungspolitik mit dem Projekt verbunden sein wird. Auswirkungen auf andere Softwareanwendungen sind jedoch nicht auszuschließen. So besteht die Gefahr, dass Softwareanwendungen auf den neuen besonders sicheren PC einer Lizenz bedürfen und dafür zusätzliche Kosten anfallen. Dadurch könnten erhebliche Marktzutrittshindernisse besonders für kleinere Softwarehersteller errichtet werden. Dies gilt in besonderem Maße für den Einsatz von quelloffener, freier Software (s. auch Antwort zu Frage 13). Insgesamt sind Auswirkungen des Palladium/TCPA-Projekts auf die Kostenstruktur für Soft- und Hardware und damit eine Verteuerung der IT-Technologie wahrscheinlich.

11. Welche wettbewerbs- und kartellrechtlichen Auswirkungen sind nach Ansicht der Bundesregierung zu erwarten?

Die Unsicherheit für künftige Auswirkungen gilt auch für die kartellrechtlichen Fragen. Dem Bundeskartellamt liegen zurzeit keine Beschwerden von Soft- oder Hardwareherstellern vor. Das in der Antwort des Parlamentarischen Staatssekretärs beim Bundesminister für Wirtschaft und Arbeit, Gerd Andres, auf die Schriftliche Frage der Abgeordneten Dr. Martina Krogmann vom 26. November 2002 Ausgeführte gilt weiterhin: Die Zusammenarbeit von Chipherstellern in der von Intel angeführten Initiative „Trusted Computing Platform Alliance“ ist nur in den vom deutschen bzw. europäischen Kartellrecht gezogenen Grenzen zulässig. Auch für die Microsoft AG gelten bei einer in das Windows-Betriebssystem integrierten proprietären Software wie dem Palladium-Programm entsprechende Schranken des Kartellrechts.

12. Wird TCPA/Palladium Auswirkungen nach Einschätzung der Bundesregierung auf die Zahl der Arbeitsplätze in den kleinen und mittleren Unternehmen der Soft- und Hardware-Branche haben?

Der Bundesregierung liegen derzeit keine gesicherten Erkenntnisse über die positiven oder negativen Beschäftigungswirkungen von TCPA/Palladium auf die mittelständischen Unternehmen des deutschen Hard- und Softwaresektors vor. Vertreter dieser Branche werden auf dem o. g. Symposium zu Wort kommen. Im Übrigen wird Bezug auf die Antwort auf die Frage 11 genommen.

13. Welche Auswirkungen könnten nach Ansicht der Bundesregierung TCPA/Palladium auf Open-Source-Software haben?

Sofern durch bestimmte Systemkomponenten ein Zwang zum Einsatz von zertifizierter Software (Anwendungsprogramme, Betriebssystem) hergestellt wird, könnte dies zu einer Behinderung der Entwicklung von Open-Source-Software (u. a. durch die Abhängigkeit von Zertifizierungsstellen) und bei dem Austausch von Dokumenten führen.

Die konkreten wirtschafts-, insbesondere die wettbewerbspolitischen Konsequenzen einer solchen Entwicklung können von hier aus noch nicht in ihrer Gesamtheit abgeschätzt werden. Die Behandlung dieses Themas ist im Rahmen des in der Antwort zu Frage 8 angesprochenen Symposiums, zu dem auch Vertreter der deutschen „Open Source“-Bewegung eingeladen werden, ebenfalls vorgesehen.

14. Wie wirkt sich TCPA/Palladium längerfristig auf die Kompatibilität mit den mit Open-Source-Software ausgerüsteten Rechnern der Bundesverwaltung und mit den auf ihnen erstellten Inhalten aus?

Unverzichtbare Voraussetzung für den Einsatz von „Palladium“ in der Bundesverwaltung ist die vollständige Kontrolle über alle vorgesehenen Sicherheitsmechanismen und Schnittstellen. Dies bedeutet insbesondere, dass Software, die für die Nutzung der von „Palladium“ vorgesehenen Funktionen notwendig ist, von der Bundesverwaltung verifiziert werden muss. Nur unter diesen Voraussetzungen kann auch mittelfristig die Kompatibilität mit den mit OSS ausgerüsteten Rechnern der Bundesverwaltung und mit den auf ihnen erstellten Inhalten gewährleistet werden.

15. Ist nach Auffassung der Bundesregierung TCPA-konforme Hard- und Software für den Einsatz in sicherheitsrelevanten Bereichen geeignet und zulässig?

Nachdem noch keine entsprechenden Realisierungskonzepte vorliegen, ist eine Aussage zu dieser Frage nicht möglich. Das in der Antwort auf die Frage 14 ausgeführte gilt hier in besonderem Maße.

16. Wenn nein, welche Maßnahmen für diesen Bereich fasst die Bundesregierung angesichts einer zunehmenden Marktpenetration von TCPA-konformer Hard- und Software ins Auge?

Siehe Antwort zu Frage 15.

17. Wie beurteilt die Bundesregierung die Einschätzung, dass diese Entwicklung durch Marktpenetration zu einem faktischen Standard führen könnte?

Der Bundesregierung liegen derzeit keine gesicherten Erkenntnisse über die Entwicklung eines faktischen Standards durch die TCPA vor. Eine Standardisierung dieser Hardwareplattform dürfte nach gegenwärtigem Erkenntnisstand vielmehr im Rahmen der Anmeldung der technischen TCPA-Spezifikationen als „Protection Profile“ zu erwarten sein (s. auch Antwort auf Frage 18).

18. Ist der Bundesregierung bekannt, wer die Hard- und Software wie zu welchem Preis zertifiziert, und wenn nein, welche Anstrengungen hat sie bisher unternommen, entsprechende Erkenntnisse zu gewinnen?

Sicherheitsstandards werden zur Registrierung bei der International Standardisation Organisation (ISO) angemeldet. Eine Zertifizierung dieses Standards kann durch jede vom Bundesamt für Sicherheit in der Informationstechnik anerkannte Prüfstelle erfolgen. Noch unklar ist allerdings das spätere Verhältnis von der entsprechenden TCPA-Zulassung und der Microsoft-Lizensierungspolitik für Soft- und Hardwareanbieter. Probleme können sich ergeben, wenn hierdurch Marktzutrittsschranken errichtet werden. Hierzu gibt es derzeit noch keine gesicherten Aussagen der Beteiligten.

19. Wie beurteilt die Bundesregierung die Auswirkungen für die Durchsetzbarkeit von Nutzungs- und Verwertungsrechten für die Anbieter digitaler Inhalte?

20. Wie verhält sich hierzu nach Ansicht der Bundesregierung die Schrankenregelung der so genannten Privatkopie?

Der Bundesregierung ist bewusst, dass die Anbieter urheberrechtlich geschützter digitaler Inhalte eine deutliche Verbesserung der Durchsetzbarkeit ihrer Nutzungs- und Verwertungsrechte von der neuen Technologie erwarten. Die zukünftige Entwicklung wird zeigen, ob diese Technologie vom Markt angenommen werden wird und sich damit die Hoffnungen der Anbieter erfüllen.

Die Bundesregierung hat im Übrigen bereits in ihrem Bericht zu den Fragen des Rechtsausschusses auf der Grundlage des Antrags der Fraktion der FDP „Die Zukunft gehört der Individuallizenz – Vergütungsregelungen für private Vervielfältigungen im digitalen Umfeld“ (Bundestagsdrucksache 14/5577) darauf hingewiesen, dass es nicht unproblematisch erscheint, wenn technische Schutzmechanismen verwendet werden, die die Möglichkeit eröffnen, den jeweiligen Nutzer zu identifizieren und ggf. elektronisch die Seh- und Hörgewohnheiten eines Nutzers zu ermitteln. Dies birgt die Gefahr des Missbrauchs in sich (Risiko des „gläsernen Nutzers“). Die Bundesregierung wird daher eingehend prüfen, ob hier über die bestehenden Regelungen insbesondere des Teledienstedatenschutzgesetzes hinaus zusätzliche gesetzgeberische Maßnahmen erforderlich sind.

Die Bundesregierung hat ferner in der Begründung zu dem Entwurf eines Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft (Bundestagsdrucksache 15/38) klargestellt, dass sie die Frage der Durchsetzung der Privatkopieschranke bei der Anwendung technischer Schutzmaßnahmen nicht mit diesem Entwurf regelt. Diese Frage bedarf vielmehr weiterer Prüfung und soll gesondert mit allen Betroffenen, den Ländern, der Rechtswissenschaft sowie der Rechtspraxis weiter intensiv und ohne Zeitdruck erörtert und im Rahmen eines weiteren Gesetzgebungsverfahrens entschieden werden.

21. Wie beurteilt die Bundesregierung Bedenken von Datenschützern, dass die auf Servern externer Kontrollinstanzen hinterlegten Daten missbraucht werden können?

22. Wie beurteilt die Bundesregierung Bedenken von Datenschützern, dass der Anwender die alleinige Kontrolle über die Funktionen des eigenen Computers mit TCPA/Palladium verliert?

Wenn (zentrale) Server einer externen Kontrollinstanz genutzt werden, um mit entsprechend modifizierten Client-Betriebssystemen Prüf- und Kontrollfunktionen zu steuern, muss sich der Anwender beim Schutz sensibler Daten uneingeschränkt auf die Vertrauenswürdigkeit dieser externen Instanz verlassen können.

Die Bedenken der Datenschützer werden daher – abhängig von der Realisierung von TCPA bzw. „Palladium“ – geteilt, da es bisher bereits viele erfolgreiche Hacking-Angriffe auf externe Server gegeben hat, bei denen Daten dann nicht Berechtigten in die Hände gefallen sind. Andererseits kann das TCPA- bzw. „Palladium“-Konzept einen erhöhten Schutz vor unberechtigtem Zugriff bieten.

Es wird die Gefahr gesehen, dass der Umgang mit Dokumenten ausschließlich gemäß den Vorgaben der externen Kontrollinstanz zulässig sein könnte und somit eine sehr weitgehende Zensur ermöglicht werden könnte.

Hard- und Software sollten daher so entwickelt und hergestellt werden, dass ausschließlich der Anwender die vollständige Kontrolle über die von ihm genutzte Informationstechnik hat.

23. Wie beurteilt die Bundesregierung Bedenken von Datenschützern, dass andere Institutionen oder Personen an vertrauliche und persönliche Informationen gelangen könnten, die im Zusammenhang mit TCPA/Palladium auf externen Servern angelegt werden, ohne dass der Anwender dies merkt?

Sofern bei dem TCPA/Palladium-Konzept, das zur Realisierung gelangt, Daten auf externen Servern abgelegt werden, besteht grundsätzlich das Risiko, dass andere Institutionen oder Personen sich vertrauliche Informationen von zentralen Servern beschaffen, ohne dass der Anwender dies bemerkt.

Die Nutzung von Hard- und Software und der Zugriff auf Dokumente muss auch weiterhin möglich sein, ohne dass Dritte davon Kenntnis erhalten und ohne dass Nutzungsprofile angelegt werden können.

24. Worin liegt nach Auffassung der Bundesregierung der Vorteil von TPM/Palladium für E-Government-Lösungen?

Für E-Government-Anwendungen ist es erforderlich, die Bürgerinnen oder den Bürger zu authentifizieren, und nicht einen Rechner zu identifizieren. Es werden daher keine speziellen Vorteile für E-Government-Anwendungen gesehen.

25. Birgt TPM/Palladium nach Ansicht der Bundesregierung auch Nachteile für E-Government, und wenn ja, welche?

Es ist nicht auszuschließen, dass die in Frage 22 geäußerten Befürchtungen zu einer Zurückhaltung auch bei der Nutzung von E-Government-Angeboten führen könnten.

26. Nimmt die Bundesregierung Befürchtungen ernst, dass durch diese Technologie einzelne, überwiegend ausländische Unternehmen mittelfristig eine signifikante Kontrolle über Systeme und Daten von Unternehmen und Behörden in Deutschland erhalten könnten?

Die Bundesregierung hat derzeit keinen sachlich begründeten Anlass zu derartigen Befürchtungen. Sie ist sich jedoch bewusst, dass bislang nur wenige deutsche Unternehmen Mitglied in der TCPA sind und dass dieser Zusammenschluss von US-Unternehmen dominiert wird. Die Bundesregierung ist sich der industrie- und sicherheitspolitischen Bedeutung dieser Entwicklung für Deutschland bewusst und sie wird deshalb das weitere Vorgehen des TCPA-Konsortiums sowie das „Palladium“-Projekt weiterhin aufmerksam beobachten.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 13 20, 53003 Bonn, Telefon (02 28) 3 82 08 40, Telefax (02 28) 3 82 08 44
ISSN 0722-8333