Deutscher Bundestag **Drucksache 15/660**

15. Wahlperiode 17. 03. 2003

Kleine Anfrage

der Abgeordneten Dr. Martina Krogmann, Günter Nooke, Bernd Neumann (Bremen), Renate Blank, Dr. Peter Gauweiler, Volker Kauder, Dr. Günter Krings, Dr. Norbert Lammert, Vera Lengsfeld, Heinrich-Wilhelm Ronsöhr, Andreas Scheuer, Dr. Ole Schröder, Erika Steinbach, Christian Freiherr von Stetten, Edeltraut Töpfer, Wolfgang Zeitlmann und der Fraktion der CDU/CSU

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

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 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.

Wir fragen die Bundesregierung:

1. Welche Maßnahmen trifft das Bundesamt für Sicherheit in der Informationstechnik (BSI) bezüglich TPM/Palladium?
2. Wann und zu welchem Zweck wurde eine entsprechende Arbeitsgruppe am BSI gegründet?
3. Wie viele Mitarbeiter umfasst diese Arbeitsgruppe?
4. Welche Erkenntnisse liegen der Arbeitsgruppe bisher vor?
5. Beabsichtigt die Bundesregierung entsprechende Erkenntnisse des BSI regelmäßig zu veröffentlichen?

   Wenn ja, in welchem Zeitraum?

   Wenn nein, warum nicht?
6. Inwieweit ist der Bundesbeauftragte für den Datenschutz bereits mit der TCPA/Palladium-Problematik befasst und was ist seine Einschätzung?
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?
8. Welche wirtschaftlichen Chancen/Risiken sieht die Bundesregierung durch TCPA für die digitale Wirtschaft?
9. Welche Chancen/Risiken sieht die Bundesregierung in der Realisierung eines hardwaregestützten sicheren Betriebssystems?
10. Wie beurteilt die Bundesregierung in der Öffentlichkeit wiederholt geäußerte Befürchtungen einer möglichen restriktiven Lizenzierungspolitik für die Hard- und Software?
11. Welche wettbewerbs- und kartellrechtlichen Auswirkungen sind nach Ansicht der Bundesregierung zu erwarten?
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?

13. Welche Auswirkungen könnten nach Ansicht der Bundesregierung TCPA/Palladium auf Open-Source-Software haben?
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?
15. Ist nach Auffassung der Bundesregierung TCPA-konforme Hard- und Software für den Einsatz in sicherheitsrelevanten Bereichen geeignet und zulässig?
16. Wenn nein, welche Maßnahmen für diesen Bereich fasst die Bundesregierung angesichts einer zunehmenden Marktpenetration von TCPA-konformer Hard- und Software ins Auge?
17. Wie beurteilt die Bundesregierung die Einschätzung, dass diese Entwicklung durch Marktpenetration zu einem faktischen Standard führen könnte?
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?
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?
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?
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?
24. Worin liegt nach Auffassung der Bundesregierung der Vorteil von TPM/Palladium für E-Government-Lösungen?
25. Birgt TPM/Palladium nach Ansicht der Bundesregierung auch Nachteile für E-Government, und wenn ja, welche?
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?

Berlin, den 14. März 2003

Dr. Angela Merkel, Michael Glos und Fraktion

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