International Working Group
on Data Protection
in Telecommunications

675.33.19 6. September 2006

Arbeitspapier

**Trusted Computing, damit zusammenhängende Technologien zur digitalen Rechteverwaltung, und die Privatsphäre:
Einige Fragestellungen für Regierungen und Softwareentwickler**

- **Übersetzung –**

angenommen bei der 40. Sitzung, 5. – 6. September 2006, Berlin

Trusted Computing und die damit zusammenhängenden Technologien zur digitalen Rechteverwaltung (TC/DRM) können für die Privatsphäre viele Vorteile bringen. Verbesserte Sicherheit von Systemen, in denen personenbezogene Daten erhoben, verarbeitet und genutzt werden, ist ein lobenswertes Ziel. Jedoch ist eine informierte und verantwortungsvolle Implementierung dieser komplexen Technologien notwendig, um unabsichtliche Risiken für die Privatsphäre zu vermeiden[1].

Den Mittelpunkt der Datenschutzrisiken bildet die Einrichtung zur „Fernattestierung" („remote attestation"), einschließlich des Potenzials für einen langfristigen Mangel an Kontrolle über die Dokumente einer Organisation. So besteht z. B. eine der identifizierten Probleme in der Beeinträchtigung des Rechts eines Individuums, über seine bei einer Behörde gespeicherten personenbezogenen Daten Auskunft zu erhalten, wenn die Zugriffsrechte auf das Dokument, das diese personenbezogenen Informationen enthält, abgelaufen sind.

Spezielle Bedingungen können für Regierungen bei der Implementierung von TC/DRM-Technologien wegen ihrer gesetzlichen Verpflichtungen bestehen, die eine Archivierung vorsehen. Aus diesem Grund sind die folgenden Empfehlungen überwiegend, aber nicht ausschließlich an öffentliche Stellen gerichtet. Organisationen des Privatsektors werden in den meisten Fällen ähnliche, möglicherweise sogar gesetzlich festgelegte Verantwortlichkeiten haben.

Empfehlungen

Die Arbeitsgruppe empfiehlt, dass Regierungen die potenziellen Gefährdungen für den Datenschutz und die Langzeit-Aufbewahrung von Daten öffentlicher Stellen erwägen, die aus der unbedachten Implementierung solcher Technologien resultieren könnten. Eine Zusammenarbeit mit anderen Regierungen bei Verhandlungen mit Verkäufern (z.B. Ausschreibungen) könnte der effektivste Weg sein, diesen potenziellen Gefahren zu begegnen.

[1] Vgl. den gemeinsamen Standpunkt der Internationalen Arbeitsgruppe für den Datenschutz in der Telekommunikation „Datenschutz und Urheberrechts-Management", angenommen auf der 27. Sitzung der Arbeitsgruppe am 4./5. Mai 2000; <http://www.datenschutz-berlin.de/attachments/233/co_de.pdf>

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

Regierungen sollten Regelungen etablieren, um sicherzustellen, dass die Vorteile der „von TC/DRM-Technologien in Bezug auf Daten der Regierung nicht von unbeabsichtigten, die Privatsphäre beeinträchtigenden Effekten überwogen werden.

Regierungen sollten die Übernahmen oder Anpassung der von Neuseeland [2] entwickelten Prinzipien und Regelungen erwägen, die nachfolgend zusammengefasst sind:

Regierungen sollten TC/DRM-Technologien nicht in einer Weise implementieren, die

1. das Recht des Einzelnen auf Auskunft gefährden könnte, oder
2. die Vertraulichkeit und Integrität von Datenbeständen der öffentlichen Verwaltung gefährden könnte, oder
3. den Schutz personenbezogener Informationen gefährden könnte, oder
4. die Sicherheit von Informationssystemen der öffentlichen Verwaltung gefährden könnte.

Die Arbeitsgruppe empfiehlt Software-Entwicklern und Verkäufern von TC/DRM-Produkten und ermutigt sie dazu, sich der Herausforderung, der sich Regierungen bei der Einführung und Implementierung von „Trusted Computing“ und digitaler Rechteverwaltung gegenüber sehen könnten, bewusst zu werden. Einige dieser Probleme mögen von denen der geschäftlichen Nutzer von TC/DRM abweichen, viele von gleicher Natur sein werden. Anbieter sollten sicherstellen, dass sie in der Lage sind, Anforderungen der Regierung im Hinblick auf die Transparenz der Anwendung dieser Systeme und Anwendungen zu entsprechen.

Anbieter könnten häufig vorfinden, dass Regierungen volle Kenntnis und Zustimmung brauchen werden zu:

1. externen Behinderungen im Hinblick auf Datensätze,
2. Datenflüssen, insbesondere solchen, die mit der Erhebung personenbezogener Daten einhergehen,
3. Übermittlungen außerhalb von Regierungssystemen (einschließlich Attestierung und anderen Hintergrundübermittlungen),
4. Regelungen, die den Zugriff auf Informationen öffentlicher Stellen kontrollieren und erlauben, und
5. Datensicherheitsrisiken im Zusammenhang mit schädlichen Inhalten wie z B. Viren und jeglichen anderen Einflüsse auf die Datensicherheit.

Anbieter sollten darauf vorbereitet sein, Regierungen unabhängige Bestätigungen darüber vorzulegen, dass ihre Systeme in der Weise funktionieren, wie es in der Spezifikation beschrieben ist.

[2] New Zealand State Services Commission: Trusted Computing and Digital Rights Management Principles and Policies, Version 1.0, 25. September 2006.