

PRESSEINFORMATION

Gegen Abschottung des chinesischen Marktes für Kryptografie-Produkte

TeleTrust fordert abgestimmtes Vorgehen der deutschen IT-Sicherheitsindustrie / Internationale Normen gegen nationale Alleingänge / Wettbewerbsverzerrung und uneinheitliches Schutzrechtsverständnis kontraproduktiv

Berlin, 08. Februar 2010 - Nach Informationen aus EU-Kreisen muss davon ausgegangen werden, dass China beabsichtigt, "Maßnahmen für Informationssicherheit" als Teil einer nationalen Initiative zur "Steigerung der Sicherheit der Bevölkerung und der staatlichen Institutionen auf allen Ebenen" umzusetzen. Dies betrifft insbesondere auch den Bereich IT-Sicherheit, der als integraler Teil der staatlichen Sicherheit angesehen wird. Die IT-sicherheitsbezogenen Maßgaben bestehen aus einem komplexen Bündel veröffentlichter und nicht-öffentlicher Richtlinien, Gesetze und Regularien, darunter auch solche zum Thema "Verschlüsselung". Es können kaum Zweifel an der Absicht bestehen, diese Maßgaben stringent durchzusetzen und IT-Sicherheit verstärkter staatlicher Kontrolle zu unterwerfen. Die Kernelemente für die Implementierung dieser Strategie sind Auditierung und Klassifizierung technischer Systeme, Produkte und Dienstleistungen, gestützt auf Konformitätsanforderungen. Beispiel für ein solches Klassifizierungsschema ist das "Multi-Layer-Protection-Scheme (MLPS)".

Dabei sollte beachtet werden, dass China aus Erfahrungen der Vergangenheit lernt, im Besonderen aus Bemühungen, die nicht in Gänze den politischen angestrebten Erfolg gebracht haben (Beispiele: Chinesischer Standard für "Wireless Communication Security" - WAPI -; Filter-Software "Green Dam"). China hat daraus die Schlussfolgerung gezogen, einen nachhaltigen, umfassenden Sicherheitsansatz zu verfolgen, mündend in strikte Auflagen, aus denen sich Konsequenzen für das Engagement der deutschen IT-Sicherheitsindustrie auf dem chinesischen Markt ergeben können.

Die deutsche IT-Sicherheitsindustrie ist darüber besorgt, dass in den Bereichen, die von China als sensitiv für die nationale Sicherheit angesehen werden, der Marktzugang erschwert bis unmöglich werden könnte, bzw. dass als Zugangsvoraussetzung geistige Eigentumsrechte an China transferiert werden müssten, die dann zu einem Entstehen starker chinesischer Konkurrenz führen könnten. Die Besorgnis, nicht nur unter deutschen IT-Sicherheitsvertretern, speist sich daraus, dass unter dem Titel "Nationale Sicherheit" Grundprinzipien des internationalen Handels unterminiert werden. Die Branche sieht sich betroffen von den von chinesischer Seite geplanten Regulierungen, wengleich auch einige der Maßnahmen bislang auf Freiwilligkeit der Unterziehung beruhen, wie in Treffen zwischen europäischen und chinesischen Regierungsvertretern klargestellt wurde:

1) Zertifizierung für kryptografische Produkte:

Gemäß den derzeit bekannten Zertifizierungsregeln des chinesischen OSCCA ("Office of State Commercial Cryptography Administration") sind ausländische Unternehmen von der Möglichkeit zum Beispiel der OSCCA-Zertifizierung ausgenommen, was sie von der Marktteilnahme in weiten Bereichen faktisch ausschließt, da diese Zertifizierung für viele Produktkategorien vorgeschrieben ist.

2) Neue Zolltarifklassifizierung für kryptografische Produkte:

Diese neuen Zolltarife ermöglichen die Identifizierung kryptografischer Produkte und deren Aus-dem-Verkehr-ziehen, wenn sie die vorgeschriebenen nationalen Zertifizierungen nicht aufweisen.

3) Offenlegung von Software:

Um bestimmte Zertifizierungen zu erlangen, müssen Sicherheitsschlüssel, Software-Design und Teile des Source Codes offengelegt werden, was nach Ansicht der Industrie nicht nur die Sicherheit der Produkte beeinträchtigen, sondern auch ein Know-how-Leck sein kann.

Diese Maßnahmen legen die Vermutung nahe, dass es neben den Überlegungen zur nationalen Sicherheit auch um die Stärkung der chinesischen nationalen IT-Industrie und um eine Abschottung des einheimischen Marktes, oder im Gegenzug um die Erlangung fremden Know-hows geht.

TeleTrusT unterstützt ausdrücklich die Aktivitäten der supranationalen standardsetzenden Institutionen, die darauf gerichtet sind, an die Stelle von nationalen Alleingängen konsensbasierte internationale Normen zu setzen, wie beispielsweise die ISO 'Common Criteria' oder den AES-Standard (ISO-Norm). TeleTrusT befürwortet die koordinierenden Bemühungen der Internationalen Normungsorganisationen (ISO/IEC) und des Europäischen Komitees für Normung (CEN bzw. CENELEC). Nationale Abschottung durch Normung und Konformitätsbewertung muss vermieden werden. TeleTrusT fordert ein abgestimmtes Vorgehen der deutschen IT-Sicherheitsindustrie sowie die Unterstützung der Bundesregierung in dieser Frage.

TeleTrusT Deutschland e.V.

Der IT-Sicherheitsverband TeleTrusT Deutschland e.V. wurde 1989 gegründet, um verlässliche Rahmenbedingungen für den vertrauenswürdigen Einsatz von Informations- und Kommunikationstechnik zu schaffen. TeleTrusT entwickelte sich zu einem bekannten Kompetenznetzwerk für IT-Sicherheit, dessen Stimme in Deutschland und Europa gehört wird. Heute vertritt TeleTrusT rund 100 Mitglieder aus Industrie, Wissenschaft und Forschung sowie öffentlichen Institutionen. In Projektgruppen zu aktuellen Fragestellungen der IT-Sicherheit und des Sicherheitsmanagements tauschen die Mitglieder ihr Know-how aus. TeleTrusT äußert sich zu politischen und rechtlichen Fragen, organisiert Messen und Messebeteiligungen und ist Träger der "European Bridge CA" (Bereitstellung von Public-Key-Zertifikaten für sichere E-Mailkommunikation) sowie des Zertifikates "TeleTrusT Information Security Professional"(T.I.S.P.). Hauptsitz des Verbandes ist Berlin.

Kontakt:	Pressekontakt:
Dr. Holger Mühlbauer	Sebastian Thümmel
TeleTrusT Deutschland e.V.	index Agentur für strategische
Bundesgeschäftsstelle	Öffentlichkeitsarbeit und Werbung GmbH
Chausseestraße 17	Zinnowitzer Str. 1
10115 Berlin	10115 Berlin
Tel.: + 49 30 / 40 05 43 10	Tel.: +49 30 / 390 88-190
holger.muehlbauer@teletrust.de	s.thuemmel@index.de
www.teletrust.de	www.index.de

