Das Risiko Trusted Computing für die deutsche Versicherungswirtschaft

Von Dr. Philipp Kramer/Marko Rogge

Positionspapier des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V.

Das Positionspapier des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V. fasst prägnant und dennoch umfassend zusammen, welche wirtschaftlichen und weiteren Interessen bei der Einführung von Trusted Computing auf dem Spiel stehen und zu berücksichtigen sind.

Trusted Computing (auch Trusworthy Computing), initiiert von wichtigen Hard- und Softwareherstellern (Promoter sind AMD, Hewlett-Packard, IBM, Intel Corporation, Microsoft, Sony Corporation, Sun Microsystems), bedeutet Absicherung von Hardware und der auf ihr gespeicherten Daten mittels Hardwarechip. Dieser Chip ist einer fest eingebauten Smartcard vergleichbar. Zum Trusted Computing gehören auch softwarebasierte Datensicherheitsmaßnahmen. Es geht um das Ziel, sicherzustellen, ob die Trägerplattform, das Betriebssystem und die ablaufenden Anwendungen trusted (vertrauenswürdig) sind. Damit sollen die Ziele der Datensicherheit, Vertraulichkeit, Integrität, Verfügbarkeit und Prüfbarkeit, umgesetzt werden.

Zugleich handelt es sich damit um eine Technik, die verhindert, dass User die laufenden Anwendungen manipulieren können, die wiederum abgesichert mit dem Softwarehersteller und untereinander kommunizieren können. Dahinter steckte ursprünglich in erster Linie Digital Right Management.

Die Beurteilung des Positionspapiers fällt sehr kritisch aus. Zunächst ist schon die Datenschutzkonformität dieser Technik zweifelhaft. Die Einführung von Trusted Computing öffnet den Herstellern unter Umständen Zugriff auf die Daten des Unternehmens. Handelt es sich um personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes, hängt die Übermittlung an den Dritten, den betreffenden Hard- und Softwarehersteller, nur noch davon ab, ob dieser bestimmte Daten tatsächlich abruft. Denn ein Übermitteln liegt bereits vor, wenn ein Dritter zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft (§ 3 Absatz 4 Nr. 3 Buchstabe b BDSG). Für diese Übermittlung liegt jedoch kein rechtfertigender Tatbestand vor. Schon für das betroffene Unternehmen ist überhaupt nicht transparent, ob ein solcher Abruf erfolgt. Das gilt erst recht für den betroffenen Dateninhaber. Ein Rechtfertigungsgrund im Sinne der allgemeinen Rechtfertigungsnorm des § 28 BDSG ist nicht ohne weiteres ersichtlich.

Erfolgt tatsächlich ein Abruf von personenbezogenen Daten durch den betreffenden Hard- und Softwarehersteller, bedeutet dieser Abruf im Zweifel daher eine unrechtmäßige Datenübermittlung durch das Unternehmen, welches die personenbezogenen Daten sonst rechtmäßig verwaltet. Die auf den ersten Blick der Datensicherheit des Unternehmens dienende Technik des Trusted Computing kann sich also bei genauerer Betrachtung schnell als eine

mit einem Bußgeld von EUR 250.000,00 bewehrte Datenübermittlung darstellen.

Das Positionspapier zeigt sehr deutlich und übersichtlich die Einstiegsgeschichte in die Thematik des Trusted Computing. Die technischen Beschreibungen helfen dem Leser, schnell die Bedeutungen von Worten wie Palladium (Microsofts Standard für die Software-Implementation), NGSCB (Microsofts neuer Standard) und Safer Computing und LaGrande (Intel) zu verstehen, so sie sie noch nicht kennen. Die Autoren haben mit viel Mühe Details recherchiert, die aufzeigen, wie gering der Sicherheitsgewinn und wie hoch die Sicherheitsrisiken und der Kontrollverlust für die Versicherungswirtschaft sind. Die technische Umstellung bei Hard- und Software setzen nach Ansicht der Autoren ein hohes Maß an Vertrauen gegenüber den Initiatoren voraus.

In den einzelnen Abschnitten dieses Papiers wird die Gefahr von Abhängigkeiten gegenüber den Produkten und der Verantwortung der Initiatoren aufgezeigt. Im einzelnen werden neue Plattformen geschaffen, die Trusted Computing unterstützen und fördern. Hierdurch werden Versicherungsunternehmen zu neuen Investitionen gezwungen. Auch ein Zugewinn an Sicherheit, der an sich mittels Trusted Computing erreicht werden soll, wird aufgezeigt. Jedoch ist derzeit eine effektive Steigerung der Sicherheit nicht erkennbar, so die Autoren. Durch Ausweitung unterschiedlicher Technologien aus dem Bereich Trusted Computing ist es kaum noch möglich, eine effiziente Kontrolle über eigene Systeme zu erhalten.

Die Autoren kommen zu dem Schluss, dass eine Umsetzung von Trusted Computing in der aktuellen Form aus Datenschutz- und Datensicherheitsaspekten nicht zu rechtfertigen ist. Es besteht die begründete Gefahr, dass Trusted Computing dazu führt, dass die Kontrolle über einen Rechner von seinem Inhaber auf denjenigen übergeht, dessen System und/oder Software der User verwendet. Zudem droht die Verletzung von Datenschutzvorschriften verletzt.

Die Broschüre, auch für anderen Unternehmen hilfreich, ist unentgeltlich erhältlich beim Gesamtverband der Deutschen Versicherungswirtschaft e.V. in Berlin (per E-Mail h.borchardt@gdv.org, per Fax 030-2020-6628 oder - vom GDV angekündigt - per Download unter www.gdv-online.de). Weitere Informationen der Trusted Computing Kampagne finden sich unter „www.trustedcomputinggroup.org“

Der ganze Artikel:
Erschienen/Erscheint im Datenschutz-Berater (Ausgabe 10/04), Handelsblatt Fachverlag, Düsseldorf. http://www.datenschutz-berater.de