

PRESSEMITTEILUNG

TeleTrusT: Sicherheitslücken bei Smartphones sind Haftungsrisiko für Telekommunikationsdienstleister

Berlin, 10.08.2011 – Für Sicherheitsrisiken bei Smartphones ist die Mehrheit der Deutschen nicht sensibilisiert. Vor diesem Hintergrund müssen Gerätehersteller die Sicherheit mobiler Endgeräte als pro-aktive Verpflichtung betrachten. Denn im Schadensfall haben die Betroffene Rechte.

Lediglich 38 % der Befragten halten zum Beispiel Datenverschlüsselung während der Nutzung mobiler Geräte für notwendig. Jeder Fünfte ist der Meinung, es gebe keine besonderen Sicherheitsmaßnahmen, die im Umgang mit mobilen Geräten berücksichtigt werden müssten. Zu diesem Ergebnis kommt die repräsentative Verbraucher-Umfrage "Mobile Geräte im Alltag" von Steria Mummert Consulting und dem Marktforschungsunternehmen Toluna, bei der 1.000 Bundesbürger befragt wurden.

Die Haftung für Schäden aufgrund von Sicherheitslücken obliegt nach Auffassung von Datenschutzrechtsexperten grundsätzlich durchaus dem "Datenverarbeiter". Sofern allerdings, wie in den häufigsten Fällen, ein Angreifer zwischen Nutzer und Telekommunikationsdatenverarbeiter tritt, um vorsätzlich und missbräuchlich Daten zu erlangen, ist dieser Dritte haftbar und schadenersatzpflichtig.

Dennoch sollte § 7 Bundesdatenschutzgesetz (BDSG) beachtet werden: "Fügt eine verantwortliche Stelle dem Betroffenen [...] einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadenersatz verpflichtet." Der betroffene Kunde eines Telekommunikationsanbieters kann sich also an die für den Datenmissbrauch verantwortliche Stelle wenden.

Gravierende Sicherheitslücken müssen unverzüglich behoben werden, woran die Telekommunikationsdienstleister schon wegen der Vermeidung von Imageschäden wirtschaftliches Interesse haben sollten. Ferner müssen Betroffene über bekanntgewordene "Datenpannen" informiert werden, insbesondere dann, wenn ein Missbrauchsrisiko besteht.

Anwendbar ist das Recht des Ortes, an dem die Datenverarbeitung stattfindet, sowie nach dem Sitz des Datenverarbeiters. Um bei Telekommunikationsdienstleistern mit Sitz im Ausland zu ermitteln, inwieweit deutsches Datenschutzrecht anwendbar ist, muss im Einzelfall geprüft werden, ob die angegriffenen Daten in Deutschland erhoben und erfasst wurden.

ca. 2.300 Zeichen

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. Heute umfasst TeleTrusT mehr als 110 Mitglieder aus Industrie, Wissenschaft, Forschung und öffentlichen Institutionen sowie Partnerorganisationen aus Deutschland und Europa. 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 Veranstaltungen und Veranstaltungsbeteiligungen und ist Trägerorganisation 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. TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI).

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