PRESSEMITTEILUNG (28/05)
Bundesbeauftragter für den Datenschutz

Bonn, den 18. August 2005

Schaar: Datenvermeidung ist der beste Datenschutz

Angesichts der zunehmenden Gefährdungen der IT-Sicherheit und der jüngsten Bedrohungen durch Computerviren begrüßt der Bundesbeauftragte für den Datenschutz Peter Schaar den heute vorgestellten Plan zum Schutz der Informationsinfrastrukturen. Ein wirksamer Schutz der Informationsinfrastrukturen ist eine Grundvoraussetzung für einen effektiven Datenschutz. Dies allein reicht aber nicht aus. Zur Prävention gehört ein sparsamer Umgang mit personenbezogenen Daten. Hierzu können sowohl die Wirtschaft, der Staat und auch die Betroffenen selbst beitragen.

Peter Schaar: „ Den besten Datenschutz erreichen wir, wenn personenbezogene Datensammlungen von vornherein vermieden werden."

Die Wirklichkeit sieht aber häufig anders aus:

Beim elektronischen Geschäftsverkehr und dem millionenfachen Einsatz von Kunden-, Geld- und Kreditkarten entstehen riesige Bestände personenbezogener Daten, die einen hohen wirtschaftlichen Wert darstellen. Dies fordert geradezu dazu heraus, die einmal angefallenen Daten auch jenseits des gesetzlich Erlaubten gewinnträchtig zu verwerten und sich gegebenenfalls illegal zu beschaffen. Die Grundsätze von Datenvermeidung und Datensparsamkeit sind deswegen hier besonders strikt zu beachten, um Begehrlichkeiten erst gar nicht entstehen zu lassen.

Aber auch dort, wo die Wirtschaft auf die Verarbeitung personenbezogener Daten verzichtet, hat dies nicht unbedingt zur Folge, dass tatsächlich weniger Daten erhoben und gespeichert werden. So wird derzeit über eine Verpflichtung der Telekommunikationsunternehmen nachgedacht, die vom Fernmeldegeheimnis geschützten Verkehrsdaten vorsorglich für staatliche Zwecke zu speichern, auch wenn sie diese selbst nicht benötigen. Dies hätte zur Folge, dass viele Millionen Datensätze der Nutzer des Internets und anderer Telekommunikationsdienste standardmäßig gespeichert werden, von denen die übergroße Mehrzahl auch für die Strafverfolgung nicht erforderlich sind.

Ein weiteres Beispiel, wo durch die Erhebung vieler personenbezogener Daten ein zusätzliches Sicherheitsrisiko entsteht, ist die Personalisierung von immer weiteren Lebensvorgängen. Besonders kritisch ist die Personalisierung der WM-Tickets. Rechtlich problematisch ist hier insbesondere die Erhebung und Verarbeitung der Pass- bzw. Personalausweisnummer.

Gefährdungen für die IT-Sicherheit kommen aber nicht immer nur von außen.
Nicht vergessen werden dürfen Sicherheitslücken, die einen Missbrauch von Daten durch eigene Mitarbeiter ermöglichen. Diesbezügliche Anforderungen an die Datensicherheit werden zum Teil auch von staatlichen Stellen nicht eingehalten. So wurde für das Programm zur Berechnung des Arbeitslosengeldes II (A2LL) bis heute keine Beschränkung durch ein differenziertes Zugriffsberechtigungskonzept eingerichtet. Das heißt, die Sachbearbeiter haben nach wie vor die

Möglichkeit eines bundesweiten Zugriffs auf den gesamten Datenbestand von A2LL. Missbräuchliche Zugriffe können mangels Protokollierung der lesenden Zugriffe nicht einmal verfolgt werden.

Bundesbeauftragter für den Datenschutz
Pressestelle
Husarenstraße 30, 53117 Bonn
Tel.: 01888-7799-916, Fax: 01888-7799-551 www.datenschutz.bund.de