

»Ein Leben ohne Datenverarbeitung ist nicht möglich«

Linden (gbp). Folgendes Szenario: Jemand erkrankt an Diabetes. Die Krankenkasse recherchiert das Konsumverhalten des Patienten und stellt fest: »Bei Ihrer Lebensweise haben Sie die Krankheit selbst verursacht.« Die Kasse verweigert die Zahlung.



L. Grapengeter

Noch ist dies Fiktion, denn noch sind diese Verknüpfungen von persönlichen Daten nicht erlaubt. Für den persönlichen Datenschutz zu sensibilisieren, war am Mittwoch Ziel eines Workshops mit dem Titel »Datenschutz - (kein) Thema für Sie?« in der Großen-Lindener Gaststätte »Zum Kronenwirt«. Eingeladen hatte der Verein technischer Führungskräfte Gießen, der sich vor allem die Förderung der beruflichen Weiterbildung auf die Fahnen geschrieben hat. Zweiter Vorsitzender Jörg Christ begrüßte neben den rund 20 Teilnehmern als Referenten Lutz Grapengeter, Dozent an der Staatlichen Technikerschule Weilburg.

Zunächst trugen die Teilnehmer zusammen, wer Daten über sie erhebt - von Behörden über Banken bis hin zu Firmen und dem Internet. An über 50 Stellen seien Daten über jeden gespeichert, schätzte Grapengeter. Dabei handele es sich nicht nur um allgemein zugängliche Daten wie Einträge in Telefonbüchern, sondern auch um persönliche Daten wie Geburtsdatum oder Arbeitgeber bis hin zu hochsensiblen Daten wie Vermögensverhältnisse, Gesundheit, religiöse oder politische Meinungen. »Ein Leben ohne Daten und deren Verarbeitungen ist nicht möglich«, resümierte der Referent.

Daten werden auch von staatlichen Stellen erhoben, die in dem Vortrag unter den Stichworten »Vorratsdatenspeicherung« und »Bundestrojaner« nur am Rande behandelt wurden. Während man sich der Erhebung und Speicherung von Daten durch Behörden und andere staatliche Institutionen nicht verweigern kann, hat man auf die Weitergabe und die Verwendung von Daten durch Firmen und Unternehmen mehr Einfluss. Grapengeter zeigte auf, welche Konsequenzen unbedachtes Verhalten im Alltag haben könne. So ermögliche etwa das Bezahlen mit Payback- oder Kreditkarten nicht nur Rückschlüsse auf das Konsumverhalten, die bei entsprechender Kombination der Daten zu genannten Szenarien führen können, sondern es ermögliche auch den äußerst lukrativen Handel mit Adressen: »Dabei geht es um sehr viel Geld«, sagte Grapengeter und fügte hinzu: »Schon eine einfache Adresse kostet einen Euro, mit Kontoverbindung sogar drei.«

Gefahren lauern auch im Internet: So hafte jeder Anschlussinhaber für alle Aktivitäten, die von seinem Anschluss ausgehen und hinterlasse Spuren, zum Beispiel durch seine IP-Adresse: »Anonymes Surfen ist praktisch nicht möglich«, so Grapengeter.

Jeder, der im Internet surfe, werde vielfach beobachtet. Beim Besuch von Internetseiten lesen viele Stellen unsichtbar mit. »Sie interessieren sich für den Preisvergleich und andere interessieren sich für Ihr Verhalten«. Grapengeter empfahl ein Zusatztool des Browsers »Firefox« mit dem Namen »NoScript«, das unter anderem die »Mitleser« sichtbar mache. Weitere Gefahren bergen laut Referent Netzwerke wie »Wer-kennt-wen« oder »StudiVZ«. Dort werden demnach zahlreiche Daten und Fotos von Nutzern - mehr als 15 Millionen täglich allein in Deutschland - gespeichert und anderen zugänglich gemacht. Sie sind auch wichtige Plattformen für Produktplatzierung in der Werbung. Auch ging Grapengeter auf zahlreiche Auskunfteien ein - von »Schufa« bis hin zu Personensuchmaschinen im Internet, die verstreute Informationen über Personen zusammentragen, ohne Wissen der Betroffenen. Aus diesen Informationen lassen sich neue Zusammenhänge ableiten. Und: »Eine Information, die einmal im Internet ist, kann praktisch nicht mehr entfernt werden«, warnte Grapengeter.

Abschließend gab er Tipps zum Umgang mit den eigenen Daten: so wenig wie möglich Daten über sich preisgeben, den Schutz der Daten ernst nehmen, auf Bonus- und Kundenkarten verzichten, bedenken, dass Preisausschreiben dem Adressenhandel dienen, überlegen, ob bestimmte Fotos und Texte wirklich ins Internet müssen, Wachsamkeit bei Angaben von persönlichen Daten am Telefon und auf Webseiten sowie die Verwendung sicherer Passwörter und Browser.