Gemeinsames Verständnis von Vertrauen

Patienten vertrauen Ärzten, Autofahrer ihren Autos und Bürger ihren Politikern – oder auch nicht. Wir wissen ganz gut, was Vertrauen bedeutet und in welchen Situationen es erforderlich und hilfreich ist. Aber was Vertrauen *in seinem Kern* ist, das wissen wir eigentlich nicht.

In diesem Schwerpunktheft über das Vertrauen in Anwendungen der modernen Informations- und Kommunikationstechnologie beleuchten wir das fundamentale Konzept des Vertrauens, ohne das Menschen kaum miteinander kooperieren könnten. Dazu untersuchen wir die charakteristischen Merkmale von Vertrauen aus der Sicht verschiedener Disziplinen und in verschiedenen Anwendungszusammenhängen. In über zehn Teilprojekten eines Forschungsschwerpunkts des Landes Rheinland-Pfalz arbeiten unter dem Namen „KoMePol – Kommunikation, Medien und Politik" die Disziplinen Informatik, Kommunikationswissenschaft, Politikwissenschaft und Psychologie zusammen, die in der Universität Koblenz-Landau auf verschiedene Fachbereiche verteilt sind. Dabei ist die Frage nach dem wechselseitigen Einfluss zwischen dem Vertrauen in die Kommunikationspartner und in das (elektronische) Kommunikationsmedium von zentraler Bedeutung.

Ein interdisziplinäres Referenzmodell des Vertrauens (*Grimm, Maier, Rothmund*) soll ein gemeinsames Verständnis in verschiedenen Disziplinen begründen und dabei gleichzeitig die Möglichkeit eröffnen, disziplinäre Besonderheiten zum Ausdruck zu bringen. Dazu wird das sozialwissenschaftlich begründete Modell von Mayer, Davis und Schoormann über interpersonales Vertrauen (1995) für weitergehende Fragestellungen erweitert, besonders für institutionelles Vertrauen und die Rolle des Kommunikationsmediums. Datenschutz und Privatheit (*Grimm, Bräunlich*) werden mithilfe diese Referenzmodells aufgeschlüsselt. Die einzelnen Elemente des Modells werden hinsichtlich der Grundprinzipien des Datenschutzes, nämlich Transparenz, Einwilligung, Datensparsamkeit usw., konkret ausgefüllt. Das ergibt eine neue Sicht auf das Risiko eines Missbrauchs personenbezogener Daten. Speziell für E-Partizipationsanwendungen (*Wimmer, Scherer*) wird untersucht, welche Angriffsszenarien es gibt und wie sie ggf. das Vertrauen in das Online-Beteiligungsangebot beeinflussen. Es wird gezeigt, welche Ansätze für Datenschutz und Sicherheit bei E-Partizipation nutzbar sind, um den Gefahren und Risiken der Angriffsszenarien zu begegnen und dadurch das Vertrauen in die E-Partizipationsangebote zu fördern. Von *Kehr, Rothmund, Gollwitzer* und *Füllgraf* wurde in einer repräsentativen Befragung risikoreiches Verhalten von Jugendlichen im Internet untersucht. Es wird gezeigt, dass risikoreiches Verhalten ein mehrdimensionales Konstrukt ist, dessen Facetten z. T. unabhängig voneinander sind. Aufklärung über das Internet vermindert offenbar risikoreiches Verhalten, generalisierte Vertrauensneigung dagegen scheint erstaunlicherweise nicht im Zusammenhang mit risikoreichen Verhalten zu stehen. Schließlich beschreibt *J. Maier* die Wirkung der Eurovisionsdebatte zwischen den Spitzenkandidaten des EU-Parlaments auf das Vertrauen in die Europäische Union und ihre Repräsentanten und nimmt dabei Bezug auf dasselbe Referenzmodell wie für Vertrauensbeziehungen im IT-Umfeld (etwa für den Datenschutz in der IT). Der letzte Blick gilt der kommunikationswissenschaftlichen Erforschung des Zusammenhangs zwischen dem Internet als Quelle für politische Informationen, der Wahrnehmung und Verarbeitung dieser Informationen durch Rezipienten und dem Einfluss des Vertrauens auf diese Prozesse (*Vogel, Milde, Stengel, Staab, Kling, Kunegis*).

Vertrauen beginnt mit der Wahrnehmung der Handlungsmöglichkeiten und ihrer Risiken. Übertragen auf die Datensicherheit bildet es daher eine wichtige Brücke zwischen der technischen und organisatorischen Umsetzung von IT-Sicherheit einerseits und der Aufmerksamkeit (Awareness) der Nutzer für ihre Sicherheit.

Rüdiger Grimm