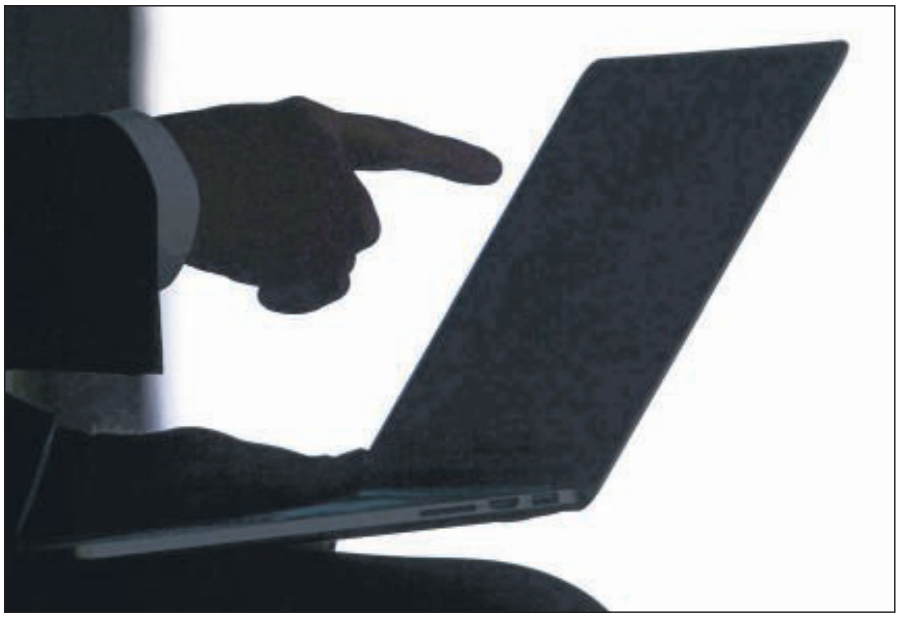
Der Schlüssel zu sicheren Daten

Wissenschaftler der Uni Kassel entwickeln Konzept zum Schutz von E-Mail-Verkehr

VON PETER DILLING

KASSEL. Die Enthüllungen des „Whistleblowers" Edward Snowden über die Abhörpraktiken des US-Geheimdienstes haben es gezeigt: Der Datenaustausch und der E-Mail-Verkehr im weltweiten Netz sind häufig nicht sicher vor unerwünschten Lauschern, die vertrauliche Informationen bei ihrem Transport vom Absender zum Empfängern abgreifen. Selbst aufwendige, auf komplizierten Algorithmen basierende Verschlüsselungstechniken, die den Inhalt einer Nachricht auf dem gesamten Weg zwischen Absender und Empfänger verbergen (End-to-End-Verschlüsselung) sollen, bieten keine hundertprozentige Garantie für Vertraulichkeit.



Schwarzen Schafen den Riegel vorschieben: Kasseler Forscher arbeiten an einem Sicherheitskonzept für E-Mail-Verkehr. Foto: Picture Alliance

Mehr Benutzerfreundlichkeit

Rechtswissenschaftler des Instituts für Wirtschaftsrecht an der Universität Kassel entwickeln nun unter Leitung von Prof. Dr. Alexander Roßnagel ein neues Sicherheitskonzept für solche End-to-End-Verschlüsselungen mit. E-Mail-Nutzer sollen dann in jedem Fall darauf vertrauen können, dass ihre Nachricht tatsächlich nur von demjenigen entschlüsselt werden kann, der sie auch erhalten soll. Außerdem sollen die Techniken, mit denen jeder Internetnutzer seine sensiblen Daten im E-Mail-Verkehr selbst schützen kann, vereinfacht werden.

Bislang werden Daten im E-Mail-Verkehr zwischen Absender und Empfänger im besten Fall durch ein komplexes System von Schlüsseln zum Ver- und Entschlüsseln, Zertifikaten und digitalen Signaturen geschützt. Doch die paarweise Verteilung der sogenannten kryptografischen Schlüssel ist eine Herausforderung. Internetnutzer bekommen diese Schlüssel auf verschiedenen Wegen und von unterschiedlichen Anbietern. Die Überprüfung, ob sie auch zum jeweiligen Kommunikationspartner passen oder noch aktuell sind, ist schwierig. „Die Systeme sind wenig benutzerfreundlich und stellen häufig nicht sicher, dass die behauptete Identität des Schlüsselinhabers auch stimmt", erklärt Stephan Blazy, wissenschaftlicher Mitarbeiter des Projekts.

Stephan Blazy

Die Wissenschaftler verfolgen den Ansatz, künftig alle Sicherheitskomponenten des E-Mail-Verkehrs mit dem Internetverzeichnisdienst (DNS) – gewissermaßen dem Adressbuch des Internets – zu verknüpfen. Dort könnten Schlüssel, Signaturen und Zertifikate zentral gespeichert und abgerufen werden.

Das neue Datensicherheitskonzept werfe allerdings auch in fast allen Rechtsgebieten Fragen auf, sagt Blazy. Beispielsweise müsse das Interesse am absoluten Schutz der eigenen Daten mit den Sicherheitsinteressen der Allgemeinheit abgewogen werden. Das ist im Bereich der Gefahrenabwehr durch Polizei und Nachrichtendienste ein besonders heikles Thema: Wer die neue Vertraulichkeit im Internet nutzt, um mit Komplizen Straftaten abzusprechen, dürfte nicht in jedem Fall Anspruch auf Geheimhaltung haben. Foto: privat/bf

HINTERGRUND

Eine Million Euro Förderung

Das auf zwei Jahre angelegte Projekt „Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln" ist Anfang 2016 gestartet. Es wird vom Bundesministerium für Bildung und Forschung mit 1,02 Millionen Euro gefördert. Für die Universität Kassel kümmert sich die Projektgruppe verfassungsverträgliche Technikgestaltung im Forschungszentrum für Informationstechnik-Gestaltung (ITeG) um das Thema. Kooperationspartner sind die Universität der Künste Berlin, der E-Mail-Anbieter mailbox.org, das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) und das Fraunhofer Institut für Sichere Informationstechnologie in Darmstadt (SIT). (pdi)