Persönliche Daten schützen
mit Privacy Enhancing Technologies

Marc Kunz
Wissenschaftlicher Assistent,
Institute for ICT-Based Management,
BFH

Dr. Annett Laube-Rosenpflanzer
Leiterin Institute for ICT-Based Management
Professorin für Informatik, BFH

Die Digitalisierung schreitet unaufhaltsam voran. Bereits heute hinterlassen wir überall Spuren im Internet. Je mehr Spuren man hinterlässt, desto grösser ist die Wahrscheinlichkeit, dass diese missbraucht werden könnten. Mit Privacy Enhancing Technologies (PET) könnten die privaten Daten besser geschützt werden.

Die heutige Welt ist digital. Je mehr wir uns im Internet bewegen, umso mehr persönliche Daten fallen an und umso mehr Spuren hinterlassen wir. Prozesse, die früher auf Papier stattfanden, werden nun elektronisch abgewickelt. Dies hat unbestritten grosse Vorteile, beispielsweise schnellere und einfachere Abwicklung oder Nachvollziehbarkeit. Im Gegenzug ist eine grössere Angriffsfläche gegeben: durch Sicherheitslücken oder durch die endlose Speicherbarkeit aller Informationen. Eine mögliche Abhilfe wird hier durch die sogenannten Privacy Enhancing Technologies (PET) geschaffen.

Was sind Privacy Enhancing Technologies?

Unter Privacy Enhancing Technologies versteht man Methoden und Systeme, die zum Ziel haben, Informationen, die Rückschlüsse auf eine Person erlauben, sog. Personally Identifiable Information (PII), besser zu schützen. Das lässt sich durch zwei Massnahmen realisieren:

1. Vermeidung der unnötigen Übertragung von Daten: Die Menge der übertragenen Daten wird auf ein Minimum beschränkt. D. h., eine Webanwendung bekommt nur die Daten, die minimal zur Erbringung des Dienstes notwendig sind.

2. Vermeidung der unnötigen Bekanntgabe von Daten: Die Form und Inhalte der Daten werden beschränkt. Ein klassisches Beispiel ist der Zugriff auf eine Dienstleistung mit Mindestalter – zum Beispiel der Kauf von Alkohol. Der Händler muss hier sicherstellen, dass der Käufer über 18 Jahre alt ist – das genaue Geburtsdatum oder das Geschlecht sind hingegen nicht nötig.

Mittels eines Anonymous Credential System (ACS) ist es einem Benutzer möglich, sich gegenüber einer anderen Partei zu identifizieren, ohne jedoch unnötig viel Information über sich preiszugeben.

Grundlagen von Anonymous Credential Systems

In der Regel arbeiten ACS auf der Basis von Pseudonymen. Die Grundidee hinter einem Pseudonym ist es, gegenüber verschiedenen Akteuren mit unterschiedlichen (Teil-)Identitäten – eben Pseudonymen – aufzutreten und somit eine Nichtverknüpfbarkeit von Zugriffen zu gewährleisten. Mehrere Dienstanbieter oder sogar mehrere Vorgänge bei einem Anbieter können somit nicht einer bestimmten Person zugeordnet werden.

Um ACS zu ermöglichen, werden auch Verfahren wie Zero Knowledge Proofs und blinde Signaturen verwendet. Zero Knowledge Proofs ermöglichen den Beweis, dass ein bestimmtes Geheimnis bekannt ist, ohne dieses jedoch offenzulegen. Blinde Signaturen ermöglichen es einem System, etwas zu bestätigen (z. B. eine Benutzerauthentifikation), ohne den Inhalt zu kennen, und verhindern damit die Wiedererkennung und auch eine mögliche Korrelation dieser Information.

Mit diesen Massnahmen ist es möglich, den Schutz der privaten Daten zu verbessern. Die Verwendung von PET werden für das Projekt Identitätsverbund Schweiz (IDV Schweiz) evaluiert. IDV Schweiz befasst sich mit dem Aufbau eines umfassenden föderierten Identitätsdienstes in der Schweiz. Ziel ist es, dass Benutzer mit dem jeweils gleichen Anmeldeverfahren auf verschiedene IT-Systeme zugreifen können.

Co-Autor
– Pascal Mainini, Wissenschaftlicher Mitarbeiter, Institute for ICT-Based Management, BFH

Kontakte
– marc.kunz@bfh.ch
– annett.laube@bfh.ch
– pascal.mainini@bfh.ch

Infos
– www.idv-fsi.ch