

Projekt AVARE: Datenschutz auf allen Endgeräten

Wissenschaftler des KIT und des FZI entwickeln Software-Anwendung, mit der sich personenbezogene Daten zentral gesteuert auf verschiedenen Endgeräten (Smartphone, Tablet, PC) schützen lassen



Funktionsweise des AVARE-Systems: AVARE kapselt die Anwendung und kontrolliert ihre Interaktion mit der Umwelt. Ein AVARE-Server verteilt die Einstellungen. (Quelle: FZI)

Smartphones, digitale Soziale Netzwerke, kommerzielle Rabattsysteme und Cloud-Anwendungen führen zur verstärkten Preisgabe personenbezogener Informationen. Diese werden teils ohne das Wissen der Bürger von multinationalen Konzernen gesammelt, gespeichert, ausgewertet und verwertet. Die Nutzer können in diesem komplexen Szenario den Schutz ihrer Daten nur schwer durchsetzen und ihre digitale Souveränität behalten. Unter Federführung des KIT entwickeln Forscher nun die Software-Anwendung AVARE, die es ermöglichen soll, die Preisgabe personenbezogener Daten zu verhindern beziehungsweise zu kontrollieren – und das parallel auf verschiedensten Endgeräten vom Smartphone über den PC bis hin zum PKW und Smart-TV.

AVARE, das steht für „Anwendung zur Verteilung und Auswahl rechtskonformer Datenschutzeinstellungen“. „Ziel des Projekts ist es, die Bürgerinnen und Bürger beim Schutz ihrer personenbezogenen Daten durch eine innovative und nutzerfreundliche Software-

Monika Landgraf
Pressesprecherin

Kaiserstraße 12
76131 Karlsruhe
Tel.: +49 721 608-47414
Fax: +49 721 608-43658
E-Mail: presse@kit.edu

Weiterer Kontakt:

Nils Ehrenberg
Pressereferent
Tel.: +49 721 608-48122
Fax: +49 721 608-43658
E-Mail: nils.ehrenberg@kit.edu

Anwendung zu unterstützen“, sagt Projektkoordinatorin Dr. Stefanie Betz vom Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) am KIT. „Die AVARE-Software soll es den Nutzern ermöglichen, ihre datenschutztechnischen Präferenzen zentral zu bestimmen und global anzuwenden. Dabei sollen die Präferenzen nach dem Eintragen an einer zentralen Stelle auf verschiedene eigene Endgeräte – etwa Smartphone, Tablet, PC, Fahrzeug oder Smart-TV sowie für verschiedene eigene Dienste wie zum Beispiel Facebook oder XING übernommen und durch technische Maßnahmen umgesetzt werden. Ein technisches Mittel zur Umsetzung des Datenschutzprofils ist zum Beispiel das Unterbinden von Zugriffen auf Datenbestände (wie z. B. Adressbuch) oder Sensoren.“

Sobald die auf dem Profil eingetragenen Nutzerpräferenzen im Widerspruch zu den gewünschten Diensten stehen, soll die AVARE-Software den Nutzer darauf hinweisen. Gleiches gilt, wenn Anbieter ihre Angebote technisch oder rechtlich – etwa durch neue Datenschutzrichtlinien – verändern. „Auf diese Weise werden die Systeme – bezogen auf deren Umgang mit personenbezogenen Daten – transparent und steuerbar, sodass auch das Vertrauen der Nutzer in die Systeme steigt“, sagt Prof. Dr. Andreas Oberweis, Direktor und Vorstand am FZI. „Die digitale Souveränität für Bürger ist bei AVARE unser oberstes Ziel.“

Ein Projekt, drei Partner, drei Jahre

Im Projekt AVARE kooperieren das Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB), das Zentrum für Angewandte Rechtswissenschaft (ZAR) – beide KIT – und das FZI Forschungszentrum Informatik in Karlsruhe. Das Projekt wird im Auftrag der Baden-Württemberg Stiftung innerhalb des Programms IT-Sicherheit durchgeführt. Es hat eine Laufzeit von drei Jahren, startete am 01. November 2015 und hat ein Volumen von 597.000 Euro.

„Für die offenen Fragestellungen des Projekts sind eine enge, fortlaufende Abstimmung und ein kooperativer Wissensaustausch unverzichtbar“, so Dr. Oliver Raabe vom ZAR. „Die technische Umsetzbarkeit und die rechtliche Zulässigkeit müssen gemeinsam betrachtet werden.“ Deshalb arbeiten in AVARE Informatiker eng mit Juristen zusammen: Das ZAR ist für die rechtswissenschaftliche Betrachtung verantwortlich. Dabei wird beispielsweise untersucht, ob ein Synallagma zwischen App-Nutzung und Zustimmung zur Datenerhebung besteht. Am FZI wird für das Projekt die prototypische Smartphone-Anwendung entwickelt und zunächst für Android

implementiert. Die Wissenschaftler des Instituts AIFB befassen sich mit der Konzeption und Nutzerevaluation der Anwendung, welche die Transparenz der über Nutzer gesammelten, gespeicherten und verwerteten Daten verbessern soll.

AVARE-SW: Vier zentrale Funktionalitäten

„Das Besondere an AVARE ist die zentrale Steuerung auf Basis eines Präferenzprofils, das der Nutzer selbst anlegt und verwaltet. Die Software unterstützt den Nutzer bei der Erstellung des persönlichen Datenschutzprofils mithilfe von für technische und juristische Laien verständlichen Erklärungen“, erläutert Stephanie Betz. „Eine weitere Besonderheit von AVARE folgt dann im zweiten Schritt, der Verteilung des Präferenzprofils.“

Denn über einen zentralen Dienst wird das Präferenzprofil auf sämtliche registrierten Endgeräte – Smartphone, PC, PKW, Tablet, usw. – verteilt. Dieser Austausch wird mittels Ende-zu-Ende Verschlüsselung abgesichert, der Schlüssel wird vom Benutzer selbst übertragen. Dadurch muss der Nutzer seine Präferenzen keinem zentralen Dienst im Klartext anvertrauen, der Schlüssel selbst wird dem zentralen Dienst nicht bekannt.

„Als dritte Funktion prüft AVARE-SW schließlich, welche anderen Anwendungen des Nutzers Daten entgegen seinem Präferenzprofil abfragen, und gibt gegebenenfalls einen entsprechenden Hinweis an den Nutzer. Initial wird dies für alle installierten Anwendungen durchgeführt“, sagt Stefanie Betz. „Danach wird dies bei jeder Neuinstallation beziehungsweise Updateinstallation einer Anwendung durchgeführt. Soweit Datenschutzvereinbarungen mit einbezogen werden können, werden auch deren Änderungen überwacht. Die Prüfung muss erneut durchgeführt werden, wenn sich die Präferenzeinstellungen des Nutzers geändert haben.“

Als vierte Funktion ermöglicht AVARE-SW bei Verletzungen der Präferenzen – soweit technisch möglich und rechtlich zulässig – die folgenden drei Reaktionen:

1. AVARE-SW kann anderen Anwendungen den Datenzugriff entziehen. Der Nutzer kann, nach Wunsch, einzelne Anwendungen davon ausnehmen.
2. AVARE-SW ermöglicht eine Beschränkung des Datenzugriffs auf einzelne konkrete Daten (beispielsweise Auszüge aus einem Adressbuch, nur bestimmte Felder bzw. bestimmte Kontakte) und definierte Zeitpunkte.

3. AVARE-SW ermöglicht das Erzeugen von „Ersatzdaten“ (z. B. wird eine „zufällige“ anstelle einer echten Ortsangabe zurückgegeben).

Nutzbar für Jedermann

Zum Projektende soll AVARE-SW als eine prototypische Anwendung vorhanden sein, als OpenSource Software publiziert und beispielsweise unter GPL lizenziert werden.

Das Karlsruher Institut für Technologie (KIT) verbindet seine drei Kernaufgaben Forschung, Lehre und Innovation zu einer Mission. Mit rund 9 400 Mitarbeiterinnen und Mitarbeitern sowie 24 500 Studierenden ist das KIT eine der großen natur- und ingenieurwissenschaftlichen Forschungs- und Lehreinrichtungen Europas.

KIT – Die Forschungsuniversität in der Helmholtz-Gemeinschaft

Das KIT ist seit 2010 als familiengerechte Hochschule zertifiziert.

Das FZI Forschungszentrum Informatik am Karlsruher Institut für Technologie ist eine gemeinnützige Einrichtung für Informatik-Anwendungsforschung und Technologietransfer. Es bringt die neuesten wissenschaftlichen Erkenntnisse der Informationstechnologie in Unternehmen und öffentliche Einrichtungen und qualifiziert junge Menschen für eine akademische und wirtschaftliche Karriere oder den Sprung in die Selbstständigkeit. Geführt von Professoren verschiedener Fakultäten entwickeln die Forschungsgruppen am FZI interdisziplinär für ihre Auftraggeber Konzepte, Software-, Hardware- und Systemlösungen und setzen die gefundenen Lösungen prototypisch um.

Diese Presseinformation ist im Internet abrufbar unter: www.kit.edu

Das Foto steht in druckfähiger Qualität auf www.kit.edu zum Download bereit und kann angefordert werden unter: presse@kit.edu oder +49 721 608-47414. Die Verwendung des Bildes ist ausschließlich in dem oben genannten Zusammenhang gestattet.