Fraunhofer
IESE

FRAUNHOFER-INSTITUT FÜR EXPERIMENTELLES SOFTWARE ENGINEERING IESE

DATENNUTZUNGSKONTROLLE
DATEN TEILEN, KONTROLLE BEHALTEN!

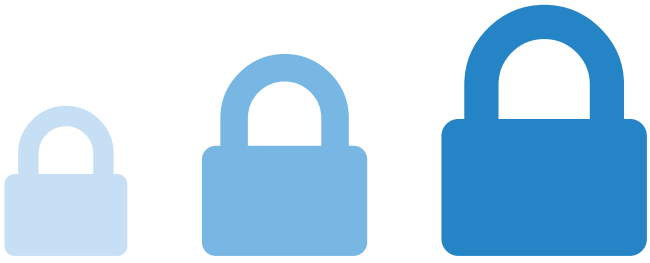
DIGITALE TRANSFORMATION UND KUNDENDATENSCHUTZ.

Moderne Geschäftsmodelle sind immer stärker datengetrieben. Das bedeutet, dass sie zunehmend auf der Verarbeitung und dem Austausch von Daten – insbesondere von Kundendaten – beruhen. Jedoch fordern sowohl Kunden als auch Justizbehörden einen umfassenden Schutz dieser Daten. Die EU-Datenschutzgrundverordnung fordert die Umsetzung verschiedener Kernprinzipien (z.B. Transparenz, ausdrückliche Zustimmung, Kontrolle der Zweckbindung). Zuwiderhandlungen können mit bis zu 4 Prozent des weltweiten Jahresumsatzes des Schuldigen bestraft werden.
Traditionelle Sicherheitslösungen stehen aber nicht im Einklang mit den heutigen Datenschutzprinzipien. Moderne Systemlandschaften sind in hohem Maße dynamisch, heterogen und großteils vernetzt. Gleichzeitig stammen viele Sicherheitskonzepte, die heutzutage noch Anwendung finden, aus den 1970er Jahren. Sie sind weder mächtig genug noch ausreichend flexibel, um im Zeitalter der fortschreitenden digitalen Transformation umfassenden Datenschutz zu gewährleisten. Mit diesen Lösungen ist es nicht möglich, die Kontrolle über Daten zu behalten, sobald einmal Zugriff auf diese gestattet wurde. Besonders die Kontrolle der Zweckbindung ist eine große Herausforderung, da dadurch die Einbindung von Drittanbieterdiensten, von denen wir alle abhängig sind, extrem behindert wird.

Neue Konzepte sind gefragt, um Kundendaten zu nutzen und sie gleichzeitig wirksam zu schützen. Das Konzept, um die vielfältigen Herausforderungen zu stemmen, nennen wir *Datennutzungskontrolle*.

Daten teilen, Kontrolle behalten

Üblicherweise regeln Sicherheitslösungen nur den Zugriff auf Daten. Das reicht aber nicht aus, um zukünftigen Missbrauch der Daten zu verhindern. Nachdem legitimer Zugriff auf die Daten gewährt wurde, muss auch die weitere Verwendung der Daten kontrolliert werden, um sicherzustellen, dass diese nur für den beabsichtigten Zweck verwendet werden. Dafür muss die Zugriffskontrolle durch eine Nutzungskontrolle ergänzt werden.



Man stelle sich beispielsweise vor, dass man sein Auto einem Freund ausleiht. Sobald man die Schlüssel aus der Hand gegeben hat, hat man komplett die Kontrolle über das Fahrzeug verloren. Unterläge das Fahrzeug einer Nutzungskontrolle, könnte man (zumindest teilweise) die Kontrolle behalten. Man könnte etwa die Höchstgeschwindigkeit begrenzen oder die Entfernung, die zurückgelegt werden darf. Natürlich besteht hierbei eine der Herausforderungen darin, das richtige Gleichgewicht zwischen Einschränkung und Nützlichkeit zu finden: Während die Geschwindigkeit in unserem Beispiel aktiv beein-

flusst werden kann, macht es keinen Sinn, das Fahrzeug sofort zu stoppen, wenn die Entfernungsgrenze erreicht ist. Aber man könnte zumindest über diesen Verstoß informiert werden und von da an die Position des Fahrzeugs verfolgen.

Im Vergleich zu Zugriffskontrollrichtlinien sind Nutzungskontrollrichtlinien wesentlich ausdrucksstärker, mächtiger und daher viel flexibler.. Dafür gibt es vier Hauptgründe: Erstens enthalten Nutzungskontrollrichtlinien nicht nur Einschränkungen, die sofort durchgesetzt werden müssen, sondern auch solche, die erst in Zukunft Anwendung finden (z.B. Löschung der Daten muss spätestens 14 Tage nach der ersten Verwendung erfolgen). Zweitens bestehen Nutzungskontrollentscheidungen nicht aus einem einfachen »Ja« (d.h. Zugriff gewähren) oder »Nein« (d.h. Zugriff verhindern). Stattdessen haben sie typischerweise die Form »Ja, aber…« (z.B. Nutzung erlaubt, aber nur, wenn personenbezogene Daten anonymisiert werden). Drittens muss, um nutzungsbasierte Entscheidungen zu treffen, der Nutzungszweck und die Nutzungssituation in Betracht gezogen werden. Es muss z.B. identifiziert werden, ob ein Nutzer eine vertrauliche Datei in einer sicheren oder in einer unsicheren Umgebung lesen will (z.B. im gesicherten Büro oder im Zug). Und schließlich müssen die Daten geschützt werden, egal, wo der Datenfluss stattfindet (z.B. Server, Desktop, Smartphone) und unabhängig von ihrer Manifestation (z.B. Datei, E-Mail, Zwischenablage).

Wo wir heute stehen

Seit über zehn Jahren ist Datennutzungskontolle ein Thema in der Forschung. Die theoretischen Grundlagen wurden inzwischen teilweise in die Praxis übertragen. Die Sprache und die Evaluierung unserer Richtlinien ist generisch und formal verifiziert. Die technische Umsetzbarkeit wurde in einer Reihe von Fallstudien mit Industriepartnern nachgewiesen.

IND²UCE bietet einen generischen und hoch skalierbaren Service, der »out-of-the-box« direkt für die Spezifizierung, Verwaltung und Evaluierung von Nutzungskontrollrichtlinien eingesetzt werden kann. Zusätzlich bietet ein einfach zu handhabendes Software Development Kit (SDK) Unterstützung für Entwickler bei der Umsetzung von Nutzungskontrolle in ihren Systemen.

IND²UCE SECURITY

Was noch zu tun bleibt

Wir müssen ein Netzwerk aus interessierten Wissenschaftlern, Entwicklern, Nutzern und Gesetzgebung schaffen, in dem wir gemeinsam auf die Standardisierung von Nutzungskontrollkonzepten und -technologien hinarbeiten. Standardisierung ist ausschlaggebend für die Gewährleistung von Kompatibilität und die Weiterentwicklung im Bereich Datennutzungskontrolle.

Fazit

Datensicherheit bedeutet mehr als nur den Zugriff zu kontrollieren. Unternehmen müssen die Nutzung von Daten kontrollieren und gleichzeitig ihre eigenen wertvollen Datenbestände und die ihrer Kunden schützen. Datenschutz ist mehr als ein Service für ihre Kunden und kein Selbstzweck: Er stellt eine gesetzliche Verpflichtung dar. Daher ist der Einsatz von Datennutzungskontrolle eine Notwendigkeit für Unternehmen, die ihre Daten schützen und deren Verwendung kontrollieren wollen.

Mit IND²UCE stellen wir eine mächtige, flexible und leicht zu handhabende Lösung für die Umsetzung von Datennutzungskontrolle bereit. Unser Team unterstützt Sie dabei, Ihre vertraulichen Daten zu schützen, indem Sie IND²UCE in Ihre Anwendungen und Netzwerke integrieren. Wenn Sie mehr über Datennutzungskontrolle und IND²UCE erfahren möchten, besuchen Sie uns unter **www.ind2uce.de** oder kontaktieren Sie uns über **ind2uce@iese.fraunhofer.de**.

Kontaktperson

Christian Jung
Abteilungsleiter
Security Engineering
christian.jung@iese.fraunhofer.de
Telefon: +49 631 6800-2146

www.iese.fraunhofer.de

Fraunhofer-Institut für Experimentelles Software Engineering IESE

Fraunhofer-Platz 1
67663 Kaiserslautern

Institutsleitung

Prof. Dr.-Ing.
Peter Liggesmeyer
Prof. Dr. Dr. h. c.
Dieter Rombach

Das Fraunhofer-Institut für Experimentelles Software Engineering IESE

Software ist Teil unseres Lebens. Eingebettet in Gebrauchsgegenstände, Wohn- und Arbeitsumgebungen oder moderne Transportmittel machen unzählige Prozessoren und Controller unseren Alltag einfacher, sicherer und angenehmer. Wir helfen Softwaresysteme zu entwickeln, auf die man sich in jeder Hinsicht verlassen kann. Die dazu erforderlichen Prozesse, Methoden und Techniken untermauern wir empirisch. Dabei legen wir Wert auf ingenieurwissenschaftliche Prinzipien wie Messbarkeit und Transparenz.

Das Fraunhofer IESE in Kaiserslautern gehört zu den weltweit führenden Forschungseinrichtungen auf dem Gebiet der Software- und Systementwicklungsmethoden. Die Produkte seiner Kooperationspartner werden wesentlich durch Software bestimmt. Die Spanne reicht von Automobil- und Transportsystemen über Automatisierung und Anlagenbau, Energiemanagement, Informationssysteme und Gesundheitswesen bis hin zu Softwaresystemen für den öffentlichen Sektor. Die Lösungen sind flexibel skalierbar. Damit ist das Institut der kompetente Technologiepartner für Firmen jeder Größe – vom Kleinunternehmen bis zum Großkonzern.

Unter der Leitung von Prof. Peter Liggesmeyer und Prof. Dieter Rombach trägt das Fraunhofer IESE seit über 20 Jahren maßgeblich zur Stärkung des aufstrebenden IT-Standorts Kaiserslautern bei. Im Fraunhofer-Verbund für Informations- und Kommunikationstechnik engagiert es sich gemeinsam mit weiteren Fraunhofer-Instituten für richtungsweisende Schlüsseltechnologien von morgen.

Das Fraunhofer IESE ist eines von 69 Instituten und Einrichtungen der Fraunhofer-Gesellschaft. Zusammen gestalten sie die angewandte Forschung in Europa wesentlich mit und tragen zur internationalen Wettbewerbsfähigkeit Deutschlands bei.

2017-03