



MYDATAÆ
CONTROL TECHNOLOGIES

Die Herausforderung

Der Austausch von Daten stellt Unternehmen vor große Herausforderungen: Auf der einen Seite müssen gesetzliche Vorgaben erfüllt werden, beispielsweise Anforderungen aus der europäischen Datenschutzgrundverordnung (DSGVO) wie Selbstbestimmung und Transparenz. Auf der anderen Seite wird der Datenaustausch mit Geschäftspartnern stets zum Risiko, sobald dieser sensible, personenbezogene oder geschäftskritische Daten beinhaltet. Sich unkontrolliert zu öffnen, birgt große Gefahren. Auf einen Austausch komplett zu verzichten, wäre jedoch kontraproduktiv und würde die Wettbewerbsfähigkeit des Unternehmens mindern. Deshalb müssen Unternehmen einen Mittelweg finden, um gleichzeitig die Chancen zu nutzen, ohne die Risiken außer Acht zu lassen.

Typische Fragestellungen

- Wie kann man Datenschnittstellen zur Laufzeit kontrollieren und verwalten?
- Wie kann man in Datenflüssen zur Laufzeit sensible, personenbezogene oder geschäftskritische Informationen effektiv filtern oder maskieren?
- Wie kann man eine einheitliche Umsetzung von Datensouveränität sicherstellen?
- Wie kann man schnell auf neue Herausforderungen bezüglich Datenschutz reagieren, ohne Änderungen in der Software vornehmen zu müssen?
- Wie kann man Datenflüsse ohne großen Aufwand anonymisieren oder verschlüsseln?

Die Lösung

Mit MYDATA Control Technologies (MYDATA) werden Unternehmen in die Lage versetzt, den intelligenten Mittelweg bei der Datenweitergabe zu beschreiten: Sie können ihre Daten vor der Weitergabe gemäß gesetzlichen Vorgaben und betrieblichen Bestimmungen filtern oder maskieren.

MYDATA ist eine technische Umsetzung von Datensouveränität, welche einen wesentlichen Baustein zur informationellen Selbstbestimmung darstellt. Sie basiert auf dem am Fraunhofer IESE entwickelten IND²UCE-Framework für Datennutzungs-

kontrolle. MYDATA setzt Datensouveränität durch einen Eingriff in sicherheitsrelevante Datenflüsse um. Dadurch wird eine feingranulare Maskierung und Filterung von Datenflüssen an Schnittstellen (APIs) ermöglicht, um diese beispielsweise zu anonymisieren. Im Vergleich zu klassischen Zugriffskontrollsystemen kann MYDATA

partielle Filterung und Maskierung der Daten, kontext- und situationsbedingte Restriktionen sowie Einschränkungen beim Verwendungszweck erzwingen. Die Einhaltung der Datensouveränität durch Veränderung von Datenflüssen wird dabei durch ein Regelwerk gesteuert.

Nutzung der Daten erlauben?

-  In der Rolle: Sachbearbeiter
-  An dem Ort: Im Büro
-  Zu dem Zweck: Abrechnung
-  Nach dem Ereignis: Freigabe
-  Mit der Häufigkeit: 10 mal in 24h

✓ **Ja**

-  Ja, aber nur 3 Tage lang
-  Ja, aber anonymisiert

⊘ **Nein**

-  Nein, und alarmieren
-  Nein, und Account sperren

Kontextbasierte Nutzungsregeln mit MYDATA

Die Vorteile von MYDATA Control Technologies

- Zentrale Services für die Verwaltung und Steuerung von Datenflüssen zur Laufzeit
- Flexibles Regelwerk zur Abbildung von Datensouveränitätsanforderungen
- Einheitliche technische Durchsetzung der Datensouveränitätsanforderungen
- Adaptives Verhalten durch Einbeziehung kontextueller Informationen
- Einfache Integration durch Open-Source SDK und ausführliche Tutorials
- Vielfältige Erweiterungsmöglichkeiten durch Plugin-Konzept

Anwendungsbeispiel 1: Datenaustausch zwischen Unternehmen (B2B)



Viele Unternehmen erkennen schon jetzt ein enormes Potenzial in der Sammlung, der Analyse und dem Austausch von verschiedensten Daten. Jedoch sehen sie beim Austausch von sensiblen Daten mit Geschäftspartnern auch ein großes Risiko. Wenn zum Beispiel ein Zulieferer

einem Unternehmen einen baldigen Lieferengpass mitteilen möchte, sollten diese Informationen nicht unkontrolliert veröffentlicht oder weiterverbreitet werden. In diesem Fall kann MYDATA sicherstellen, dass die Nutzung zeitlich beschränkt und nur durch einen berechtigten Personenkreis erfolgt. Beim Datenaustausch zwischen Unternehmen gibt es viele weitere Anforderungen hinsichtlich Datensouveränität, die MYDATA zu erfüllen hilft.

Anwendungsbeispiel 2: Datenfreigabe beim Banking (C2B2B)



Die EU-Richtlinie PSD2 (Payment Services Directive) regelt unter anderem die Teilnahme an der Zahlungsbranche durch Nichtbanken. Externe Unternehmen können hierbei Zugriff auf Transaktions- und Kundendaten erhalten, um dem Bankkunden einen Mehrwert zu bieten. PSD2-Schnittstellen mit MYDATA bieten dem Bankkunden Selbstbestimmung bei

der Datennutzung durch Dritte. Der Bankkunde bestimmt selbst, welche Transaktionsdaten an externe Unternehmen herausgegeben werden. Dazu können die Daten mit MYDATA gefiltert und maskiert werden. Bei einer Bewertung der Kreditwürdigkeit sind zwar monatliche Einnahmen und Ausgaben relevant, aber eventuell will der Bankkunde nicht alle Transaktionsdetails preisgeben. Hier schafft MYDATA mehr Vertrauen durch die Stärkung der Datensouveränität beim Bankkunden.

Anwendungsbeispiel 3: Digitalisierter ländlicher Raum (C2C)



Auch im ländlichen Raum schreitet die Digitalisierung stark voran. Die Digitale-Dörfer-Plattform (www.digitale-doerfer.de) des Fraunhofer IESE ermöglicht es Gemeinden und Kommunen, digitale Dienste für Bürger anzubieten. Es gibt zum Beispiel einen Mitbringdienst: Bürger können andere bitten, ihnen Waren aus dem regionalen Handel an die Haustür zu liefern. Diese Anfrage ist grundsätz-

lich öffentlich sichtbar. MYDATA schützt hierbei die Privatsphäre der Bürger. Nähere Details zur Lieferung, wie die exakte Lieferadresse, werden nur dem Lieferanten angezeigt. Falls der Belieferte nicht zu Hause ist, kann er einen geheimen Ablageort bestimmen. Diesen sieht der Lieferant allerdings nur auf seinem Smartphone, wenn er sich im näheren Umkreis des Lieferortes befindet. Hierbei nutzt MYDATA kontextuelle Informationen, wie den Standort des Lieferanten, um die Nutzung der Daten zu kontrollieren.

Anwendungsbeispiel 4: Data Loss Prevention im eigenen Unternehmen (B2x)



Die – meist unbeabsichtigte – Weitergabe von sensiblen Informationen ist für Unternehmen eine stetige Bedrohung. Oft passiert dies durch die Unachtsamkeit der Mitarbeiter und nicht durch Hacker oder böswillige Absicht. Ein Mitarbeiter versendet eine E-Mail an Externe und hat versehentlich ein vertrauliches, internes Office-Dokument angeheftet. Um Szenarien wie dieses zu verhindern, bieten die

MYDATA Control Office Plugins die passende Lösung. Dokumente verschiedenster Formate (u.a. Word, Excel, PowerPoint, PDF) können gemäß ihrer Vertraulichkeitsstufe klassifiziert und ihre Nutzung kontrolliert werden. MYDATA überwacht beispielsweise beim Versenden von Anhängen, dass interne Dokumente erst nach expliziter Freigabe an externe Empfänger verschickt werden. Vertrauliche Dokumente dürfen ausschließlich verschlüsselt versendet werden. MYDATA verhindert damit ungewollte Datenabflüsse.

Unsere Technologie

MYDATA Control Technologies besteht aus drei Kernfunktionen:

- **MYDATA Control Enforcement:** Für die Durchsetzung von Nutzungsregeln bietet MYDATA Kontrollpunkte an, welche einfach in Zielsysteme integriert werden können. Diese können an Datenschnittstellen Informationen filtern und maskieren. Zusätzlich bietet MYDATA die Möglichkeit, Aktionen mittels weiterer Komponenten auszuführen, wie beispielsweise eine Benachrichtigung per E-Mail. Die Funktionalität der Kontrollpunkte und Aktionsausführungen kann durch Plugins erweitert werden.
- **MYDATA Control Policies:** Zur Laufzeit können neue Regeln zur Datennutzung verfasst werden. Dabei

können unter anderem zeit- und häufigkeitsbasierte Nutzungen («Daten dürfen innerhalb eines Tages nur 5 Mal verwendet werden»), situationsbasierte Nutzungen («Sensible Daten dürfen auf Dienstreisen nicht eingesehen werden») und maskierte Nutzungen («Für den PSD2-Dienstleister werden die mittleren 12 Stellen der IBAN durch ein X ersetzt») eingestellt werden.

- **MYDATA Control Management:** MYDATA vereint die Verwaltung von Datensouveränitätsanforderungen und technischen Komponenten in einer zentralen Verwaltungsoberfläche.

Der modulare und komponentenbasierte Aufbau von MYDATA erlaubt eine einfache und skalierende Integration in beste-



Kernfunktionen von MYDATA

hende Systeme. Das Plugin-Konzept bietet eine Vielzahl von Erweiterungsmöglichkeiten, inklusive der Anbindung an andere Systeme (z.B. an Verzeichnisdienste). Hierzu stellt ein Software Development Kit mit ausführlicher Dokumentation die passende Entwicklerunterstützung zur Verfügung. MYDATA kann um drei Arten von Plugins erweitert werden:

- **Datenmodifikation:** MYDATA kontrolliert und modifiziert Datenflüsse basierend auf den aktiven Regeln. Beispielregel: »Entfernen Sie alle Kundenadressen, bevor Sie Daten an Dritte weitergeben.«
- **Aktionsausführung:** MYDATA führt (kompensierende) Aktionen basierend auf dem aktiven Regelsatz aus. Beispielregel: »Wenn jemand auf meine Daten zugreift, benachrichtigen Sie mich per E-Mail.«
- **Informationsauflösung:** MYDATA integriert verschiedene Arten von Informationsquellen, z.B. Standortdaten oder Verzeichnisinformationen. Beispielregel: »Zugriff nur erlauben, wenn der Benutzer die Rolle Administrator innehat und sich auf dem Firmengelände befindet.«

Unsere Dienstleistungen

Wir stellen Ihnen mit MYDATA Control Technologies eine effektive Softwarelösung zur Erreichung von Datensouveränität zur Verfügung. Gerne unterstützen wir Sie mit individuellen, auf Sie angepassten Dienstleistungen:

- **Potenzialanalyse:** Möchten Sie in Erfahrung bringen, welche Einsatzmöglichkeiten MYDATA zum Schutz Ihrer Daten bietet? In einem Workshop erarbeiten wir mit Ihnen gemeinsam Anwendungsszenarien für MYDATA in Ihrem Unternehmen.
- **Pilotierung:** Möchten Sie MYDATA Control Technologies in Ihrem Unternehmen testen? Unsere Entwickler unterstützen Sie gerne bei einer Proof-of-Concept-Realisierung in Ihrem Unternehmenskontext.
- **Entwicklerunterstützung:** Möchten Sie Unterstützung bei der Integration von MYDATA in Ihr System, bei der Entwicklung eigener Plugins oder bei der Spezifikation von Nutzungsregeln für Ihre Anwendungsfälle? Unsere Experten unterstützen Sie gerne bei der Lösung Ihrer individuellen Herausforderungen.

Ansprechpartner

Denis Feth
Abteilungsleiter
Security Engineering
denis.feth@iese.fraunhofer.de
Telefon +49 631 6800-2157
www.iese.fraunhofer.de

Fraunhofer-Institut für Experimentelles Software Engineering IESE

Fraunhofer-Platz 1
67663 Kaiserslautern

Weitere Informationen zu MYDATA
Control Technologies finden Sie
unter:
<https://www.mydata-control.de>



Das Fraunhofer IESE

Seit mehr als 20 Jahren ist das Fraunhofer IESE in Kaiserslautern eine der weltweit führenden Forschungseinrichtungen auf dem Gebiet der Software- und Systementwicklungsmethoden. In mehr als 1.200 Projekten haben seine wissenschaftlichen Mitarbeiter bereits ihre Kompetenzen in den Bereichen Prozesse, Architektur, Security, Safety, Requirements Engineering und User Experience eingebracht. Das Institut beschäftigt sich mit innovativen Themen wie Industrie 4.0, Big Data und Cyber-Security, ist Technologie- und Innovationspartner für die digitale Transformation in den Bereichen Autonomous & Cyber-Physical Systems und Digital Services und erforscht das Zusammenspiel von eingebetteten Systemen und Informationssystemen in digitalen Ökosystemen.

Das Fraunhofer IESE ist eines von 72 Instituten und Einrichtungen der Fraunhofer-Gesellschaft. Zusammen gestalten sie die angewandte Forschung in Europa wesentlich mit und tragen zur internationalen Wettbewerbsfähigkeit Deutschlands bei.