TOYOTA Deutschland GmbH – OEDIV SecuSys Kunde

Eine IAM Success Story

Management Summary

Die OEDIV SecuSys GmbH fokussiert ihr Geschäftsfeld auf den IT – Security-Bereich **Identity und Provisioning Management** und bietet mit IAM Softwarelösung die flexible Möglichkeit, Nutzer und Berechtigungen revisionssicher und effizient zu verwalten.

Anfang des Jahres 2010 konnte die OEDIV SecuSys GmbH **TOYOTA** als neuen Kunden gewinnen - genauer gesagt die **Toyota Deutschland GmbH** (TDG). Partner der OEDIV SecuSys GmbH im Identity & Access Management Projekt ist die **Toyota Informations - Systeme GmbH** (TIS), in deren Verantwortung die IT der TDG liegt.



Toyota Deutschland GmbH

Die Geschichte von Toyota in Deutschland begann 1971 mit der Gründung der Deutschen Toyota Vertriebs GmbH in Köln, die 1974 von der Toyota Motor Corporation (TMC) übernommen und 1976 in Toyota Deutschland GmbH umbenannt wurde. Zusammen mit 25 weiteren europäischen Toyota Importeuren wurde die TDG 2005 in einer Dachgesellschaft, der heutigen Toyota Motor Europe (TME) mit Sitz in Brüssel zusammengefasst.

Den deutschlandweiten Vertrieb der Automarken Toyota und – seit 1990 – der Premium – Marke Lexus übernimmt ein gut aufgestelltes Händlernetz. Es umfasst mehr als 700 Standorte, an denen sich insgesamt über 10.000 Mitarbeiter den Wünschen und Fahrzeugen ihrer Kunden annehmen. Dabei stehen Qualität, Umweltverträglichkeit und Kundenzufriedenheit ganz oben auf der Agenda.

Vor allem die Erfahrungsberichte von Projektleitern erfolgreicher Kundenprojekte und ein Prototyp, in dem das Lösungsszenario dargestellt wurde, überzeugten den Auftraggeber, von OEDIV SecuSys GmbH als Partner die richtige Entscheidung zu treffen.


Ralf Schriddels – Manager IT Enterprise Architecture, Toyota Deutschland GmbH

Ralf Schriddels – Manager IT Enterprise Architecture – legte bei der Produktauswahl besonderen Wert auf ein mittelstandsgerechtes Tool mit größtmöglicher Flexibilität im Funktions-, Leistungs- und Serviceumfang. Es sollte eine innovative und weitestgehend „vorkonfigurierte“ SW-Lösung sein, die in einer stufenweisen Implementierung zu schnellen Projekterfolgen führt und kein kostenintensives Großprojekt im Big Bang-Verfahren.

Mit dem IdM-System soll künftig eine dezentrale und zeitnahe Pflege der Mitarbeiterdaten und Vergabe von Berechtigungen direkt bei den Autohäusern erfolgen und das TIS Service Center dadurch spürbar entlastet werden. Durch personalisierte Accounts und personen- und aufgabenbezogene Berechtigungen sollen insbesondere Datenschutz-, Sicherheits- und Compliance - Anforderungen erfüllt und die Nachvollziehbarkeit der Rechte - Vergabe ermöglicht und sichergestellt werden.

„Voraussetzung für die Erfüllung dieser Anforderungen ist eine Softwarelösung, die in der Lage ist, die komplexe Organisationsstruktur abzubilden, über ein flexibles, leistungsfähiges Rollenmodell verfügt, die Automatisierung der Prozesse in der Benutzer- und Rechteverwaltung ermöglicht und einen starken Compliance Monitor zur Verfügung stellt“ so Prof. Dr. Dr. Gerd Rossa, ehem. CEO der OEDIV SecuSys GmbH.

Kurzbeschreibung des UIM – UAM Projekt @ TDG

Im Rahmen des Projekts wurde eine zentrale Identity- und Access-Management-Struktur für das Händlernetz der Toyota Deutschland GmbH aufgebaut und in die bestehende IT-Umgebung integriert. Ziel war es, die Verwaltung von Benutzeridentitäten und Berechtigungen zu vereinheitlichen und gleichzeitig eine dezentrale Pflege der Benutzerdaten durch die einzelnen Händlerbetriebe zu ermöglichen.

OEDIV SecuSys übernahm die Konzeption des Daten- und Berechtigungsmodells sowie die technische und organisatorische Umsetzung. Dazu gehörten unter anderem die Modellierung von Rollen und Prozessen, die Integration in bestehende Systeme und die Begleitung der Einführung vor Ort.

Besonderes Augenmerk lag auf der Umsetzung von Datenschutz-, Sicherheits- und Compliance-Anforderungen sowie auf einer praxistauglichen Struktur für das gesamte Händlernetz.

Das Ergebnis: Rund 10.000 Mitarbeitende in den Toyota-Händlerbetrieben in Deutschland werden über die etablierte IAM-Struktur verwaltet.

Ausgangssituation

Bei den TOYOTA Händlern in Deutschland wird für den Zugriff auf die zentralen TOYOTA – Systeme (TDG / TME) in jedem Autohaus ein System-User verwendet, mit dem bei Bedarf die Mitarbeiter der Autohäuser in den zentralen Systemen bzw. Anwendungen arbeiten. Dies hat zur Folge dass:

- jeder User die Möglichkeit hat, alle Daten auf den Systemen einzusehen.
- alle User uneingeschränkte Rechte in den Anwendungen haben (also nicht nur solche, die sie zur Ausübung ihrer Tätigkeit effektiv benötigen)
- die User „anonym“ arbeiten
- es nicht nachvollziehbar ist, wer wann welche Zugriffsrechte erhalten und wer wann welche Aktivitäten durchgeführt hat: Mangel an Compliance
- es keine rollenbasierte Administration gibt
- bestimmte (vertrauliche) Informationen nicht elektronisch zur Verfügung gestellt werden können.

Das seitherige Vorgehen birgt erhebliche Risiken im Hinblick auf die Einhaltung von Datenschutz und Sicherheitsbestimmungen und erfüllt nicht die immer höheren Anforderungen an die Nachvollziehbarkeit und Compliance. Diese Situation verschärft sich durch:

- neue Anforderungen von TME – Applikationen, die künftig die Nutzung von personalisierten User Accounts voraussetzen
- die Vielzahl von Systemen / Applikationen im Handel mit unterschiedlichen User Repositories, für die IT Support zu leisten ist. Die User Administration im Handel / Helpdesk erfordert einen hohen Zeitaufwand
- eine prognostizierte steigende Arbeitsbelastung sowie Ressourcen-Engpässe im Helpdsk durch geplante Umstellungen

Aus den genannten Gründen steht die Verwaltung von User Accounts im Handel sowie deren Zugriffsberechtigungen im Fokus.

Es wird eine Software benötigt, die ein flexibles Rollenmodell unterstützt, die Automatisierung der Prozesse ermöglicht und den Anforderungen an Datenschutz, Sicherheit und Compliance gerecht wird. Mehrfache Initiativen zur User Identity Management Implementierung sind bisher aus verschiedenen Gründen gescheitert. Eine Eigenentwicklung bzw. Auftragsprogrammierung wird als zu zeitraubend und kostenintensiv angesehen.

Zieldefinitionen

Die Pflege der Mitarbeiterdaten und Rechtevergabe über ein Rollenmodell soll nicht wie bisher zentral, manuell und aufwendig durch eine Mitarbeiterin aus dem Bereich Händlertraining, sondern künftig **dezentral** – und damit **zeitnaher** – durch den TOYOTA Händlerbetrieb selbst erfolgen. Die Administration soll **effizienter und sicherer**, der administrative **Aufwand** im Bereich Händlertraining **deutlich geringer**, und das TOYOTA Service Center **spürbar entlastet** werden.

Durch die Einführung von **personalisierten Accounts** für das TOYOTA Händlernetz sollen insbesondere Datenschutz-, Sicherheits- und Compliance - Anforderungen erfüllt und die Nachvollziehbarkeit der Rechte - Vergabe ermöglicht und sichergestellt werden.

Von der im Händlerumfeld noch üblichen Verwendung von Gruppenusern soll zu **personen- und aufgabenbezogenen Berechtigungen** (Rollen) übergegangen werden. Die Mitarbeiter in den Autohäusern sollen nur die Rechte erhalten, die sie tatsächlich benötigen.

In Notfällen muss die TOYOTA Zentrale aber immer die Möglichkeit haben, einzugreifen und die Verwaltung in jedem Autohaus direkt zu unterstützen. Ein Antragsverfahren soll die Freigabe der Rollenzuordnungen steuern und die Nachweisbarkeit dieser Business-Prozesse sicherstellen.

Risiken

Ein Risiko ist das kaum fassbare Regelwerk der TOYOTA Händlerbetriebe, welches ein flexibles Rollenmodell voraussetzt, um die weitestgehend rechtlich eigenständigen ca. 700 Händler (Autohäuser) mit rund 10.000 Beschäftigten flexibel verwalten zu können. Es erfordert eine langjährige Erfahrung in der Rollenmodellierung, um die komplexen Anforderungen von TOYOTA hinsichtlich Integration des Händlernetzwerks erfüllen zu können.

Business Values

Durch die dezentrale Pflege der Mitarbeiterdaten und Rechtevergabe seitens der Händler soll der administrative Aufwand im Bereich Händlertraining und UHD deutlich reduziert werden. Der hohe Automatisierungsgrad und die hohe Verarbeitungsgeschwindigkeit steigern Akzeptanz und Produktivität.

Dank der Prozesssicherheit sind keine Berechtigungsleichen im System vorhanden. Messbar ist dies durch Soll/Ist-Abgleich zwischen dem IAM-System und den Zielsystemen. Dass die Mitarbeiterdaten bei der Änderung automatisch in alle Zielsysteme provisioniert werden, bringt einen deutlichen Qualitätsgewinn der Userdaten, da nur noch wenige bis keine Fehler zu verzeichnen sind.

Die genannten Soll-/Ist-Abgleiche sind, neben weiteren umfangreichen Compliance - Möglichkeiten, bereits komplett durch die Softwarelösung realisierbar.

Umsetzungsstrategie /-prozesse

Fast alle angeforderten Funktionen des IdM-Systems waren im Standard der IAM-Lösung bereits vorhanden und mussten nicht separat für das Projekt entwickelt werden. Speziell für das Projekt wurden lediglich kundenspezifische Bildungsregeln für Anmeldenamen und Systemattribute sowie Plausibilitätsprüfungen programmtechnisch umgesetzt. Bisher wurden drei wichtige Zielsysteme der TIS über Connectoren automatisch angebunden.

Um die Ziele hinsichtlich der Compliance-Anforderungen und der Revision zu erfüllen, liegt ein besonderes Augenmerk auf der Implementierung des Rollenmodells und darauf aufbauend auf der Umsetzung der Prozessmodelle.

Das Standard – Vorgehensmodell der OEDIV SecuSys GmbH (Workshop → Pilot → Projekt Phase 1 → Projekt Phase 2 → Folgephasen) wurde an die spezielle Kundensituation angepasst und ein Prototyp vorgeschaltet.

Nach erfolgreicher Pilotinstallation (mit ausgewählten Händlern) erfolgt die Produktivsetzung des gesamten Systems. Dabei wird insbesondere in der Startphase eine intensive Betreuung und Unterstützung der IAM Administration sowie eine rasche Problembearbeitung sichergestellt.

Kontakt:

OEDIV SecuSys GmbH
Kurt-Dunkelmann-Straße 2
18057 Rostock
Tel. 0381 375730