IoT-Identitätsmanagement: Integrieren Sie besser vernetzte Produkte und Services in Ihr Ökosystem

Verwalten Sie vertrauenswürdige Beziehungen zwischen Menschen, Services und Dingen für eine skalierbare digitale Transformation

Das Internet der Dinge (IoT) revolutioniert unsere Wirtschaft über nahezu alle Branchen hinweg – von der Fertigung über das Transportwesen, Smart Homes und Telekommunikation bis hin zum Gesundheitswesen.

Unternehmen, die ihre Geräte mit Systemen, Daten und Menschen vernetzen, können ihren Kunden ein stärker automatisiertes und damit personalisierteres Gesamterlebnis bieten. Gerade viele neue Geschäftsmodelle können mit IoT-basierten Services häufig mehr Umsatz generieren als mit den Produkten, über die diese Services bereitgestellt werden.

Für einen gelungenen Einstieg in IoT braucht es jedoch mehr, als Geräte irgendwie netzwerkfähig zu machen. Bei Dingen kann es sich auch um Services, Systeme, Anwendungen oder Datenquellen handeln – einfach alles, das mit einem Mensch oder einer Organisation interagiert. Die Kommunikation dieser Dinge erfolgt über die Cloud, das Mobilfunknetz, soziale Medien oder ältere Plattformen und hat den Zweck, Informationen anzufordern oder bereitzustellen, Befehle auszugeben und die Verwaltung komplexer automatisierter Prozesse zu unterstützen. Sobald die Verbindungen im IoT dichter und komplexer werden, stellen sich wichtige Fragen:

Wie können wir den Zugriff auf all diese Dinge und die gespeicherten Informationen verwalten? Wie steuern wir, welche Personen oder Geräte welche Befugnisse haben sollen? Und wie können wir unser Ökosystem als Ganzes schützen? Stellen Sie sich diesen Fragen gleich zu Beginn Ihrer IoT-Transformation, denn sobald Ihr Ökosystem an Größe und Komplexität gewinnt, wird es ungleich schwieriger, die richtigen Antworten zu finden.

Identitätsmanagement ist ein wirkungsvolles Instrument, um IoT-Ökosysteme in Unternehmensumgebungen zu verwalten und zu schützen.

Es bietet eine Grundlage für die granulare Zugriffskontrolle und Vertrauenswürdigkeit, auf der Unternehmen Berechtigungen verwalten und vertrauenswürdige Beziehungen zwischen Menschen, Services und Dingen herstellen können. Ebenso kann festgelegt werden, wofür diese Menschen, Services und Dinge Zugriffs- und Kommunikationsrechte haben, welche Befehle sie ausgeben und auf welche Daten sie zugreifen dürfen. Das Identitätsmanagement identifiziert Dinge in ihrem Kontext, sodass Unternehmen ihr IoT-Ökosystem effektiver verwalten, pflegen und erweitern können.

In diesem Whitepaper lesen Sie, welch wichtige Rolle das Identitätsmanagement im IoT-Kontext spielt und welche Anforderungen dafür erfüllt sein müssen.

Mit dem IoT-Boom rückt die Skalierbarkeit in den Fokus

IoT ist ein starker Treiber der digitalen Transformation, entsprechend schnell wächst der Markt. Vernetzte Fahrzeuge, Telemedizin, Wearables, Smart Homes und Smart Grids – all diese bahnbrechenden B2C-Geschäftsmodelle würden ohne IoT-Technologien nicht funktionieren. Dasselbe gilt für B2B-Modelle wie Smart Manufacturing, Smart Lighting und Flottenmanagement der nächsten Generation.

Je mehr Geräte, Anwendungen, Services und Menschen Teil eines IoT-Ökosystems sind, desto heterogener wird es und desto komplexer ist die Zugriffskontrolle. Beispiele für solche Systeme sind:

- Systeme wie ein Ereignisdatenspeicher, Motorsteuerungen oder ganz einfach Sensoren
- Über mehrere Steuerungen und Systeme verteilte Daten zu Nutzung, Ereignissen, individuellen Konfigurationen oder dem aktuellen Status
- Organisationen wie ein Hersteller, ein Distributor, eine Versicherungsgesellschaft oder eine Behörde
- Einzelpersonen wie interne Mitarbeiter, Mitarbeiter von Dienstleistern, Auditoren und Partner
- Ereignisse von der normalen Nutzung bis hin zu Verstößen gegen festgelegte Grenzwerte, Unfälle und technische Fehler

In diesem dynamischen Umfeld muss der Servicebetreiber jederzeit genau kontrollieren können, wer bei welchen Ereignissen Zugriff auf welche Daten erhalten darf. Der Datenfluss innerhalb des IoT muss fehlerfrei funktionieren, um ein reibungsloses digitales End-to-End-Erlebnis zu schaffen. Gleichzeitig könnten Schwachstellen bei der Sicherheit und Netzwerkkontrolle verheerende Auswirkungen haben, z. B. den Verlust persönlicher Daten, Manipulation oder das Eindringen von Schadsoftware.

Die Gewährleistung vertrauenswürdiger Beziehungen, ihre Kontrolle und Verwaltung sind bereits bei einigen Hundert oder Tausenden Geräten eine Herausforderung. In großen Unternehmen können jedoch mehrere Millionen von Dingen auf komplexeste Weise miteinander vernetzt sein. Hier stoßen manuelle Ansätzen unweigerlich an ihre Grenzen. Ein funktionierendes Identitätsmanagement mit einer automatisierten Zugriffskontrolle ermöglicht es, selbst komplexeste IoT-Ökosysteme einfach zu verwalten.

Modernes Identitätsmanagement ist der Schlüssel zu Ihrem IoT-Erfolg

Mithilfe von Identitätsmanagement wird die Zugriffskontrolle auch im großen Maßstab möglich. So kann ein Gerät beispielsweise die Erlaubnis zur Selbstinstallation bei einem Identitätsverzeichnis am Netzwerk-Edge beantragen – eine wichtige Funktion für Installationen, die zu umfangreich für ein manuelles Vorgehen sind. Ein weiteres Beispiel: Ein Techniker erhält Zugriff auf einen Sensor, um erfasste Daten abzurufen, oder der Sensor selbst verfügt über die Berechtigung, auf Anwendungen zuzugreifen und direkt Daten hochzuladen.

Moderne IoT-Anforderungen können das klassische Identitätsmanagement jedoch schnell an seine Grenzen bringen. Früher ging es bei Identitäten im Wesentlichen darum, den Zugriff auf Anwendungen und Systeme durch Menschen zu steuern. Nun stellen neue Entwicklungen ganz andere Anforderungen an das Identitätsmanagement:

- Identität bezieht sich nicht mehr ausschließlich auf Menschen. Heutzutage brauchen auch Dinge eine eigene Identität und haben untereinander komplexe Identitätsbeziehungen.
- Das Identitätsmanagement unterliegt nicht mehr der alleinigen Kontrolle durch die IT. Innerhalb eines Ökosystems gibt es viele verschiedene Anbieter und Authenticators mit jeweils eigenen Identitäts-Sets.
- Viele Benutzer verfügen entsprechend ihren aktuellen Rollen oder Aufgaben über unterschiedliche Identitäten oder Profile, zwischen denen sie je nach Bedarf wechseln. Sowohl Identität als auch Risiko können je nach Kontext variieren und erfordern mehr Flexibilität im Autorisierungsansatz.

Ein leistungsfähiges Identitätsmanagement erlaubt die Zuweisung von Identitäten nicht nur für Personen und Geräte, sondern auch für Services, welche über einen Edge-Controller oder andere Komponenten des IoT-Ökosystems bereitgestellt werden. Dadurch ist eine bessere Kontrolle über die Interaktionen zwischen Dingen und Daten möglich. Beispielsweise können unterschiedliche Berechtigungsstufen für unterschiedliche Personen und Geräte gelten. Einem Betreiber können Berechtigungen gemäß seiner spezifischen Rolle und Qualifikation zugewiesen werden. Ein externer Servicetechniker kann je nach Kontext unterschiedliche Rechte erhalten. Generell

schafft Identitätsmanagement die Voraussetzung, um Interaktionen zwischen Menschen, Organisationen und Dingen sowie deren Zugriff auf Systeme, Komponenten und Daten zu kontrollieren und zu verwalten – und dies in der Dimension und Komplexität, wie sie in IoT-Umgebungen großer Unternehmen üblich sind.

Identitätsmanagement für verschiedene IoT-Anwendungsfälle

Übergeordnet lässt sich der IoT-Markt nach zwei Anwendungsfällen unterscheiden: Optimierung und Transformation.

Business Optimization zielt darauf ab, den Wertertrag bestehender Assets und Investitionen zu maximieren, die Effizienz zu steigern und die operative Leistung zu verbessern. Instrumente sind beispielsweise prädiktive Wartung, Prozessautomatisierung, Fertigungs- sowie Gebäudeautomatisierung. Eine Organisation verwendet IoT, um eine digitale Arbeitsumgebung zu schaffen, in der ein Gesamtkontext und Vertrauenswürdigkeit herrschen. In der ersten Phase kommt IoT zum Einsatz, um die Nutzfläche, Arbeitsplätze und Assets zu optimieren. In den folgenden Phasen werden Sitzpläne mit Kontextbezug, Smart-Room-Technologien und andere Maßnahmen zur Steigerung der Teameffizienz und -produktivität eingeführt. So unterstützt Identitätsmanagement diesen Anwendungsfall:

- Erstellung einer vertrauenswürdigen Identität für neue Dinge im Netzwerk
- Herstellung vertrauenswürdiger Beziehungen zwischen den Anwendern und ihren Dingen
- Erstellung einer 360-Grad-Ansicht
- Ermöglichung eines granularen Zugriffsmanagements und Rechteübertragung

Business Transformation beinhaltet die Einführung neuer digitalen Services und Geschäftsmodelle. Während Optimierungsinitiativen nach innen wirken, zielen Transformationsprogramme darauf ab, das Kundenerlebnis zu revolutionieren. Dies gelingt durch eine stärkere Abgrenzung vom Wettbewerb, mehr Kundenzufriedenheit und -loyalität und nicht zuletzt durch mehr Umsatz.

Diese Ergebnisse kann Identitätsmanagement für diesen IoT-Anwendungsfall erzielen:

- Ganzheitliche Omnichannel-Erlebnisse, die den Kunden über verschiedene Geräte, Plattformen und Kontexte begleiten und daraus ein Umsatzplus generieren
- Stärker personalisierte Angebote, z. B. indem Kundenpräferenzen auf ein breiteres Produkt- und Servicespektrum angewendet werden, um daraus neue und potenziell bahnbrechende Geschäftsmodelle abzuleiten
- Verständnis für die Beziehungen und Interaktionen zwischen Personen, Services und Dingen in einer bestimmten Umgebung
- Sammlung vertrauenswürdiger Daten als Grundlage für hochgradig personalisierte Angebote

Ein klassisches Beispiel für ein IoT-basiertes Transformationsszenario ist ein Fahrzeughersteller, der mithilfe von IoT vertrauenswürdige Identitäten für Fahrzeuge und Geräte erstellt, um neue Mobilitätsservices anzubieten. Vorteile für den Käufer:

- Authentifizierung des Halters vor bestimmten Aktionen wie Aufschließen, Anlassen und Steuern des Fahrzeugs
- Sichere gemeinsame Nutzung durch Festlegen von maximaler Nutzungszeit, Nutzungsradius, Beschleunigung und Geschwindigkeit
- Teilen von Daten zu Fahrzeugnutzung und -status mit einem Versicherungsanbieter, um besondere Vertragsbedingungen zu verhandeln, oder mit einem Händler oder einer Werkstatt, um prädiktive Wartungsleistungen in Anspruch zu nehmen
- Remote-Erlaubnis für einen Lieferdienst, das Fahrzeug zu öffnen und ein Paket dort abzulegen
- Bezahlen an einer Tankstelle, einem Drive-In-Schalter oder einer Mautstelle auf Basis des authentifizierten Fahrers und dem zugewiesenen Zahlungsmedium

Empfehlungen für Ihren IoT-Erfolg

Das IoT-Ökosystem eines großen Unternehmens ist umfassend und komplex. Gehen Sie bei der Konzeption und Umsetzung mit Umsicht und Weitblick vor. Folgen Sie dabei dem Leitsatz: „Think big, act small, move fast“ – Groß denken, in kleinen Schritten handeln, schnell vorwärts gehen.

- **Definieren Sie eine ambitionierte, ganzheitliche Vision** für Ihre IoT-Strategie. Wie möchten Sie die Beziehung zu Ihren Kunden und deren Beziehung zu Ihren Produkten und Services neu gestalten? Welche neuen Erlebnisse können Sie auf der Grundlage Ihrer bestehenden Geschäftsmodelle schaffen? Wie sieht Ihr aktuelles Geschäft in „smart“ aus, z. B. vom Vertrieb von Beleuchtungsprodukten zu smarten Beleuchtungsservices, oder vom Fahrzeugverkauf zu smarten Mobilitätsservices? Diese Vision ist Ihr Grundgerüst, um das Sie Ihre einzelnen Initiativen und Technologien entwickeln.

- **Fangen Sie klein an,** indem Sie ein klar definiertes, bestehendes Problem mit einer relativ einfachen Lösung beheben. Wenn Sie dadurch Erfahrungen gesammelt haben, gehen Sie die nächsten Schritte in Richtung Ihrer Leitvision.
- **Bauen Sie ein starkes Netzwerk** an Technologie-Partnern auf. Die IoT-Implementierung kann nicht im Alleingang gelingen! Nach einer von James Brehm & Associates durchgeführten Studie sind in ein großes IoT-Projekt in der Regel acht Systeme oder Unternehmen involviert.
- **Schaffen Sie keine Silos,** während Sie Ihr IoT erweitern. Sie könnten Sie bei der späteren Digitalisierung Ihrer Geschäftsprozesse ausbremsen.
- **Erzielen Sie schnelle Ergebnisse,** um die Vorteile der Initiative in der Praxis aufzuzeigen, sich die Unterstützung aller Beteiligten zu sichern und schnell vom Optimierungs- und Transformationspotenzial Ihres IoT zu profitieren.

Modernes Identitätsmanagement von ForgeRock für ein erfolgreiches IoT

ForgeRock bietet Unternehmen ein solides Fundament für ein erfolgreiches IoT. Es weist Identitäten zu, definiert Beziehungen und gewährleistet die Vertrauenswürdigkeit zwischen allen Elementen im Ökosystemen.

- Die ForgeRock-Technologien für identitätsbasierte Sicherheit nach innen und außen haben ihre Leistungsfähigkeit bereits bei der Bereitstellung von über einer Milliarde Identitäten unter Beweis gestellt.
- Eine zentrale, einheitliche Plattform bricht Silos auf, spart Kosten ein und beschleunigt die Markteinführung neuer Funktionen.
- Dank der nahtlosen Integration in die bestehende Infrastruktur können Unternehmen ihre Umgebung voll nutzen und sie gleichzeitig um neue IoT-Funktionalität erweitern.
- Die API-Integration in neue und bestehende Geschäftsprozesse verhilft Unternehmen zu mehr Automatisierung, Effizienz und Kontrolle.

Die ForgeRock Identity Platform ist auf eine Vielzahl unterschiedlicher IoT-Anwendungsfälle ausgelegt, unter anderem:

- Erstellen und Speichern von Identitäten für Smart Devices
- Authentifizieren von Smart Devices für einen Cloud-Service
- Zugangsberechtigung für Smart Devices zu Cloud-APIs
- Selbstregistrierung und IoT-Benutzeridentität
- Individualisierung des Benutzererlebnisses im IoT
- Aufheben von Verknüpfungen zwischen Geräte- und Benutzeridentitäten
- Schutz von IoT-Ressourcen

Fazit

Das IoT erweitert und beschleunigt die digitale Transformation, indem es neue Services, Geschäfts- und Betriebsmodelle für Unternehmen in nahezu jeder Branche ermöglicht. IoT-Installationen in großen Unternehmen sind dringend auf ein effektives Instrument angewiesen, um die Interaktionen und Datenflüsse zwischen Dingen und Einheiten zu kontrollieren und vertrauenswürdige Beziehungen innerhalb des Ökosystems aufzubauen. Identitäten bieten die Möglichkeit, die Zugriffskontrolle in der Struktur des Ökosystems zu verankern. Es werden ausschließlich autorisierte Aktionen und Datenzugriffe durch authentifizierte Einheiten zugelassen. Dabei kann es sich um einen Betreiber, einen externen Techniker, ein System oder eine Anwendung oder sogar um einen Datenstrom handeln. Ein identitätsbasiertes, alle Organisationen und Systeme eines Unternehmens umfassendes Ökosystem gibt dem Unternehmen mehr Freiheit und Flexibilität bei der Gestaltung seiner Services. So kann es sich stärker vom Wettbewerb abheben, die Kundenzufriedenheit steigern und betriebliche Abläufe optimieren. Eine leistungsfähige Identitätsmanagementlösung bietet einem Unternehmen die beste Grundlage für eine kontinuierliche Optimierung von Qualität und Skalierbarkeit seiner Services.

Erfahren Sie hier, wie ForgeRock vertrauenswürdige Beziehungen zwischen Menschen, Services und Dingen verwaltet.