Grundsätze des IoT

April 2016

Hinweise

Dieses Dokument wird nur zu Informationszwecken zur Verfügung gestellt. Es stellt das aktuelle Produktangebot und die Praktiken von AWS zum Erstellungsdatum dieses Dokuments dar. Änderungen vorbehalten. Kunden sind für ihre eigene unabhängige Einschätzung der Informationen in diesem Dokument und jedwede Nutzung der AWS-Services verantwortlich. Jeder Service wird „wie besehen“ ohne Gewähr und ohne Garantie jeglicher Art, weder ausdrücklich noch impliziert, bereitgestellt. Dieses Dokument gibt keine Garantien, Gewährleistungen, vertragliche Verpflichtungen, Bedingungen oder Zusicherungen von AWS, seinen Partnern, Zulieferern oder Lizenzgebern. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden werden durch AWS-Vereinbarungen geregelt. Dieses Dokument gehört, weder ganz noch teilweise, zu den Vereinbarungen von AWS mit seinen Kunden und ändert diese Vereinbarungen auch nicht.

Inhalt

Kurzbeschreibung

Dieses Whitepaper legt die Grundsätze dar, die beim Entwickeln einer Strategie für das Internet of Things (IoT) beachtet werden sollten. Das Whitepaper hilft Ihnen dabei zu verstehen, welche Vorteile die Amazon Web Services (AWS) haben und wie die AWS Cloud-Plattform die kritische Komponente sein kann, die die Grundsätze einer IoT-Lösung unterstützt. Das Whitepaper gibt auch einen Überblick über die AWS-Services, die Bestandteil einer IoT-Gesamtstrategie sein sollten. Dieses Whitepaper richtet sich an Entscheidungsträger, die sich über Internet of Things-Plattformen informieren wollen.

Übersicht

Eines der Wertangebote einer Internet of Things- (IoT-) Strategie ist die Möglichkeit, Einblicke in Zusammenhänge zu gewähren, die zuvor für das Geschäft nicht sichtbar waren. Aber bevor ein Unternehmen eine Strategie für das IoT entwickeln kann, braucht es eine Plattform, die die Grundprinzipien einer IoT-Lösung erfüllt.

AWS ist der Überzeugung, dass einige grundlegende Freiheiten die organisatorischen und wirtschaftlichen Vorteile der Cloud für Unternehmen nutzbar machen. Diese Freiheiten sind der Grund, warum über eine Million Kunden die AWS-Plattform bereits nutzen, um praktisch jede beliebige Cloud-Arbeitslast zu unterstützen. Diese Freiheiten sind auch der Grund, warum die AWS-Plattform sich als der primäre Katalysator für jede Internet of Things-Strategie bei kommerziellen, industriellen und Verbraucherlösungen erweist.

AWS-Kunden, die in einem solchen Lösungsspektrum arbeiten, haben die Grundsätze erfasst, die für den Erfolg jeder IoT-Plattform entscheidend sind. Diese Grundsätze sind Agilität, Umfang, Kosten und Sicherheit. Es hat sich gezeigt, dass diese Faktoren für den langfristigen Erfolg jeder IoT-Strategie von wesentlicher Bedeutung sind.

In diesem Whitepaper sind diese Grundsätze wie folgt definiert:

- Agilität – die Freiheit, Geschäfte und technische Initiativen ohne Einschränkungen schnell zu analysieren, auszuführen und aufzubauen
- Umfang – die nahtlose regionale oder globale Erweiterung von Infrastruktur, um betriebliche Anforderungen zu erfüllen

- Kosten – das Verstehen und Kontrollieren der Kosten für den Betrieb einer IoT-Plattform
- Sicherheit – sichere Kommunikation vom Gerät über die Cloud bei gleichzeitigem Aufrechterhalten von Compliance und schnellem Iterieren

Durch den Einsatz der AWS-Plattform können die Unternehmen agile Lösungen entwickeln, die an das exponentielle Wachstum der Geräteanzahl angepasst werden können, die Möglichkeit zur Kostenverwaltung bieten und gleichzeitig auf einer der sichersten Datenverarbeitungs-Infrastrukturen der Welt aufgebaut sind. Ein Unternehmen, das eine Plattform auswählt, die diese Freiheiten bietet und diese Grundsätze fördert, verbessert seine organisatorische Ausrichtung auf die Unterscheidungsmerkmale seines Geschäfts und den strategischen Wert, Lösungen innerhalb des Internet of Things zu implementieren.

Grundsätze des IoT

Agilität

Ein wichtiger Vorteil, den Unternehmen beim Erstellen einer IoT-Lösung erlangen wollen, ist die Fähigkeit, Geschäftsmöglichkeiten wirkungsvoll quantifizieren zu können. Diese Geschäftsmöglichkeiten werden aus zuverlässigen Sensordaten, Ferndiagnosen sowie Fernbefehlen und -steuerungen zwischen Nutzern und Geräten abgeleitet. Unternehmen, die diese Metriken erfolgreich sammeln, öffnen die Tür zum Überprüfen verschiedener geschäftlicher Hypothesen, die auf ihren IoT-Daten basieren. So können Hersteller beispielsweise Predictive Analytics-Lösungen aufbauen, um langfristig den idealen Wartungszyklus für ihre Produkte zu messen, zu testen und einzustellen. Der IoT-Lebenszyklus besteht aus mehreren Phasen, die erforderlich sind, um große Flotten von physischen Geräten zu beschaffen, herzustellen, zu integrieren, zu testen, bereitzustellen und zu verwalten. Beim Entwickeln physischer Geräte treten in dem kaskadenartigen Prozess Herausforderungen und Reibungskräfte auf, die die geschäftliche Agilität verlangsamen können. In Verbindung mit den Investitionskosten für Hardware und der Entwicklung und Bereitstellung physischer Komponenten in großem Maßstab führen diese Reibungskräfte oft zu der Notwendigkeit, die Geräte über längere Zeiträume in Gebrauch zu lassen, um die notwendige Kapitalrendite (ROI) zu erreichen.

Bei den ständig wachsenden Herausforderungen und Möglichkeiten, mit denen Unternehmen heute konfrontiert sind, ist der IT-Bereich ein wichtiger Wettbewerbsfaktor, der die Geschäftsleistung, Produktentwicklung und Geschäftstätigkeiten unterstützt. Damit die IoT-Strategie eines Unternehmens Wettbewerbsvorteile bietet, benötigt die IT-Organisation eine Vielzahl von Tools, die die Kompatibilität innerhalb der IoT-Lösung und unter einer heterogenen Mischung von Geräten fördern. Unternehmen, denen es gelingt, erfolgreich eine Ausgewogenheit zwischen den kaskadenartigen Prozessen von Hardware-Freigaben und den agilen Methoden der Software-Entwicklung zu erreichen, können ständig den Wert optimieren, der sich aus ihrer IoT-Strategie ableitet.

Skalierbarkeit und globale Präsenz

Zusätzlich zu dem exponentiellen Wachstum der Anzahl verbundener Geräte kommuniziert jedes der *Dinge* im Internet of Things Datenpakete, die eine zuverlässige Konnektivität und einen Speicher von hoher Haltbarkeit erfordern. Bevor es Cloud-Plattformen gab, schafften die IT-Abteilungen zusätzliche Hardware an und unterhielten zu wenig genutzte, zu viel bereitgestellte Kapazität, um die steigende Menge an Daten bewältigen zu können, die von den Geräten gesendet wurde, auch als Telemetrie bekannt. Durch das IoT ist eine Organisation mit der Herausforderung konfrontiert, die immense Anzahl an Netzwerkverbindungen von diesen verstreuten, verbundenen Geräten zu verwalten, zu überwachen und zu sichern.

IoT-Lösungen erfordern nicht nur die Skalierung und den Ausbau einer Lösung an einem regionalen Standort, sondern auch die Fähigkeit, global und an verschiedenen physischen Standorten zu skalieren. IoT-Lösungen sollten an mehreren physischen Standorten bereitgestellt werden, um die Geschäftsziele einer globalen Enterprise-Lösung zu erfüllen, z. B. Daten-Compliance, Datenunabhängigkeit und geringere Kommunikationslatenz für eine bessere Reaktionsfähigkeit der Geräte im Feld.

Kosten

Oft liegt der größte Wert einer IoT-Lösung in den Telemetrie- und Kontextdaten, die von den Geräten generiert und gesendet werden. Der Aufbau einer lokalen Infrastruktur erfordert Vorab-Investitionen in Hardware; dabei kann es sich um größere, feste Ausgaben handeln, die nicht direkt mit dem Wert der Telemetrie korrelieren, die ein Gerät irgendwann in der Zukunft produziert. Um die Notwendigkeit, Telemetrie heute zu erhalten, mit einem unbestimmten Wert abzugleichen, der aus den biometrischen Daten in der Zukunft abgeleitet ist, sollte eine IoT-Strategie eine elastische und skalierbare Cloud-Plattform nutzen. Bei der AWS-Plattform zahlt ein Unternehmen nur für die Services, die es nutzt, ohne dass ein langfristiger Vertrag erforderlich ist. Ein flexibles, nutzungsbasiertes Preismodell erlaubt direkten Zugriff auf die Kosten einer IoT-Lösung und die damit verbundene Infrastruktur. Hinzu kommt der geschäftliche Nutzen, der sich durch die Aufnahme, Verarbeitung, Speicherung und Analyse der Telemetrie durch diese IoT-Lösung ergibt.

Sicherheit

Die Grundlage einer IoT-Lösung beginnt und endet mit der Sicherheit. Da die Geräte große Mengen sensibler Daten senden und die Endbenutzer von IoT-Anwendungen außerdem die Möglichkeit haben können, ein Gerät direkt zu steuern, muss die „Security of Things“ ein durchgängiges Konstruktionselement sein. IoT-Lösungen sollten nicht nur im Hinblick auf Sicherheit entwickelt werden, sondern Sicherheitskontrollen enthalten, die jede Schicht der Lösung durchdringen. Sicherheit ist keine statische Formel; IoT-Anwendungen müssen in der Lage sein, bewährte Sicherheitspraktiken ständig zu modellieren, zu überwachen und zu iterieren. Beim Internet of Things ist die Angriffsfläche anders als bei der traditionellen Web-Infrastruktur. Die Durchgängigkeit der allgegenwärtigen Datenverarbeitung bedeutet, dass IoT-Schwachstellen zu Bedrohungen führen könnten, die Todesfälle zur Folge haben, beispielsweise bei einem gefährdeten Steuerungssystem für Erdöl-Pipelines oder Stromnetze.

Eine im Wettstreit stehende Dynamik bei der IoT-Sicherheit ist für physische Geräte und die eingeschränkte Hardware für Sensoren, Mikrocontroller, Aktuatoren und eingebettete Bibliotheken von entscheidender Bedeutung. Diese Einschränkungsfaktoren können die Sicherheitsfunktionen begrenzen, die die einzelnen Geräte ausführen können. Mit dieser zusätzlichen Dynamik müssen IoT-Lösungen ständig ihre Architektur, Firmware und Software anpassen, um den sich ändernden Sicherheitsanforderungen einen Schritt voraus zu sein. Obwohl die Einschränkungsfaktoren von Geräten höhere Risiken, Hindernisse und potenzielle Kompromisse zwischen Sicherheit und Kosten darstellen können, muss der Aufbau einer sicheren IoT-Lösung für jede Organisation das primäre Ziel sein.

AWS-Services für IoT-Lösungen

Die AWS-Plattform bietet eine Grundlage für die Ausführung einer agilen, skalierbaren, sicheren und kostengünstigen IoT-Strategie. Um den geschäftlichen Nutzen zu erreichen, den das IoT einer Organisation bringen kann, sollten Sie die Breite und Tiefe von AWS-Services bewerten, die häufig in umfassenden, verteilten IoT-Bereitstellungen verwendet werden. AWS bietet eine Reihe von Services an, um die Produkteinführungszeit zu verkürzen: von der SDK-Unterstützung für eingebettete Software bis zur Datenverarbeitung in Echtzeit und ereignisgesteuerten Datenverarbeitungsservices.

In den nächsten Abschnitten behandeln wir die in IoT-Anwendungen am häufigsten verwendeten AWS-Services und erläutern, wie diese Services die Grundsätze einer IoT-Lösung erfüllen.

AWS IoT

Das Internet of Things kann nicht ohne *Dinge* existieren. Jede IoT-Lösung muss zuerst eine Verbindung herstellen, um mit den Geräten interagieren zu können. AWS IoT ist ein von AWS verwalteter Service, der dazu dient, große Flotten von Geräten für eine Anwendung zu verbinden, zu verwalten und zu betreiben. Die Kombination aus Skalierbarkeit der Konnektivität und Sicherheitsmechanismen für die Datenübertragung innerhalb von AWS IoT bildet die Grundlage für die IoT-Kommunikation als Bestandteil einer IoT-Lösung. Wenn Daten an AWS IoT gesendet worden sind, kann eine Lösung ein Ökosystem aus AWS-Services nutzen, das Datenbanken, Mobile-Dienste, Big Data, Analysen, Machine Learning und vieles mehr umspannt.

Device Gateway

Ein Device Gateway hat die Aufgabe, die Sitzungen und Abonnements für alle verbundenen Geräte in einer IoT-Lösung in Stand zu halten. Das AWS IoT-Device Gateway ermöglicht eine sichere, bidirektionale Kommunikation zwischen verbundenen Geräten und der AWS-Plattform über MQTT, WebSockets und HTTP. Kommunikationsprotokolle wie MQTT und HTTP erlauben es einem Unternehmen, industrielle Standardprotokolle statt firmeneigener Protokolle zu nutzen, die die zukünftige Kompatibilität einschränken würden.

Als Publish/Subscribe-Protokoll begünstigt MQTT schon an sich skalierbare, fehlertolerante Kommunikationsmuster und fördert eine Vielzahl von Kommunikationsoptionen zwischen den Geräten und dem Device Gateway. Diese Nachrichtenmuster reichen von der Kommunikation zwischen zwei Geräten bis hin zu Übertragungsmustern, bei denen ein Gerät eine Nachricht über ein gemeinsames Thema an eine große Gruppe von Geräten senden kann. Darüber hinaus stellt das MQTT-Protokoll verschiedene Ebenen von Servicequalität (QoS) bereit, um die Rückübertragung und Zustellung von Nachrichten zu kontrollieren, während sie an die Abonnenten veröffentlicht werden. Die Kombination aus Veröffentlichen und Abonnieren gibt mit QoS den IoT-Lösungen nicht nur die Möglichkeit zu kontrollieren, wie die Geräte mit einer Lösung interagieren, sondern macht es auch berechenbarer, wie Nachrichten zugestellt, bestätigt und im Fall von Netzwerk- oder Gerätefehlern erneut gesendet werden.

Shadows, Device Registry und Rules Engine

AWS IoT bietet zusätzliche Funktionen, die für den Aufbau einer robusten IoT-Anwendung entscheidend sind. Der AWS IoT-Service beinhaltet die Rules Engine, die vom Device Gateway empfangene Nachrichten filtern, umwandeln und weiterleiten kann. Die Rules Engine verwendet eine SQL-basierte Syntax, die Daten aus Nachrichten-Nutzlasten auswählt und aufgrund der Merkmale der IoT-Daten Aktionen auslöst. AWS IoT bietet auch einen Geräte-Shadow, der eine virtuelle Darstellung eines Geräts projiziert. Der Geräte-Shadow fungiert als Nachrichtenkanal, um Befehle zuverlässig an ein Gerät senden zu können, und speichert den letzten bekannten Zustand eines Geräts in der AWS-Plattform.

Um den Lebenszyklus einer Flotte von Geräten zu verwalten, hat AWS IoT eine Geräte-Registry. Die Geräte-Registry ist der zentrale Ort zum Speichern und Abfragen einer zuvor definierten Reihe von Attributen der einzelnen Dinge. Die Geräte-Registry unterstützt die Erstellung einer ganzheitlichen Verwaltungsansicht einer IoT-Lösung, um die Verbindungen zwischen Dingen, Shadows, Berechtigungen und Identitäten zu steuern.

Sicherheit und Identität

Für verbundene Geräte sollte eine IoT-Plattform über den gesamten Entwicklungszyklus der Hardware und Software die Konzepte von Identität, geringsten Rechten, Verschlüsselung und Autorisierung verwenden. AWS IoT verschlüsselt den Datenverkehr zum und vom Service über Transport Layer Security (TLS) mit Unterstützung für die meisten größeren Cipher Suites. Zur Identifizierung muss sich ein verbundenes Gerät bei AWS IoT mit einem X.509-Zertifikat authentifizieren. Jedes Zertifikat muss auf einem Gerät bereitgestellt, aktiviert und installiert sein, damit es bei AWS IoT als gültige Identität verwendet werden kann. Zur Unterstützung dieser Trennung von Identität und Zugang für die Geräte stellt AWS IoT für die Geräteidentitäten IoT-Richtlinien bereit. AWS IoT verwendet auch AWS Identity and Access Management- (AWS IAM-) Richtlinien für AWS-Benutzer, -Gruppen und -Rollen. Durch die IoT-Richtlinien hat eine Organisation Kontrolle über die Kommunikation, indem der Zugriff auf bestimmte IoT-Themen entsprechend der Identität eines bestimmten Gerätes erlaubt oder verweigert werden kann. Die AWS IoT-Richtlinien, -Zertifikate und AWS IAM sind für eine explizite, zugelassene (Whitelist-) Konfiguration der Kommunikationskanäle aller Geräte im AWS IoT-Ökosystem eines Unternehmens ausgelegt.

Ereignisgesteuerte Services

Um die Grundsätze von Skalierbarkeit und Flexibilität in einer IoT-Lösung zu erreichen, sollte eine Organisation die Techniken einer ereignisgesteuerten Architektur nutzen. Eine ereignisgesteuerte Architektur fördert eine skalierbare und entkoppelte Kommunikation durch die Erstellung, Speicherung, Nutzung und Reaktion auf Ereignisse von Interesse, die in einer IoT-Lösung vorkommen. Nachrichten, die in einer IoT-Lösung generiert werden, sollten zuerst kategorisiert und einer Serie von Ereignissen zugeordnet werden. Die IoT-Lösung sollte anschließend diese Ereignisse mit Geschäftslogik verknüpfen, die Befehle ausführt und eventuell zusätzliche Ereignisse im IoT-System generiert. Die AWS-Plattform stellt mehrere Anwendungsservices zum Aufbau einer verteilten, ereignisgesteuerten IoT-Architektur bereit.

Durch ihren Aufbau bedingt, verfügen ereignisgesteuerte Architekturen über die Fähigkeit, Ereignisse dauerhaft zu speichern und an ein Ökosystem interessierter Abonnenten zu übertragen. Zur Unterstützung der entkoppelten Ereignisorchestrierung stellt die AWS-Plattform mehrere Anwendungsservices bereit, die eine zuverlässige Ereignisspeicherung und hoch skalierbare, ereignisgesteuerte Datenverarbeitung gewährleisten. Eine ereignisgesteuerte IoT-Lösung sollte zum Erstellen einfacher und komplexer Ereignis-Workflows Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS) und AWS Lambda als grundlegende Anwendungskomponenten nutzen. Amazon SQS ist ein schneller, beständiger, skalierbarer und vollständig verwalteter Warteschlangenservice. Amazon SNS ist ein Web-Service zum Veröffentlichen von Meldungen aus einer Anwendung und zum sofortigen Zustellen an Abonnenten oder andere Anwendungen. AWS Lambda dient dazu, Code als Reaktion auf Ereignisse auszuführen, während die zugrunde liegenden Computerressourcen automatisch verwaltet werden. AWS Lambda kann Meldungen direkt von anderen AWS-Services empfangen und darauf reagieren. In einer ereignisgesteuerten IoT-Architektur wird AWS Lambda dort eingesetzt, wo die Geschäftslogik ausgeführt wird, um zu ermitteln, wann interessante Ereignisse im Kontext eines IoT-Ökosystems aufgetreten sind.

AWS-Services wie Amazon SQS, Amazon SNS und AWS Lambda können den Konsum von Ereignissen von der Verarbeitung und Geschäftslogik trennen, die auf diese Ereignisse angewendet werden. Diese Trennung von Verantwortlichkeiten sorgt in einer End-to-End-Lösung für Flexibilität und Agilität. Diese Trennung erlaubt die schnelle Änderung von Ereignistrigger-Logik oder der Logik, die zum Aggregieren kontextbezogener Daten zwischen Teilen eines Systems verwendet wird. Darüber hinaus erlaubt diese Trennung, dass Änderungen in eine IoT-Lösung eingegeben werden, ohne den kontinuierlichen Strom von Daten zu unterbrechen, die zwischen den Endgeräten und der AWS-Plattform hin- und hergesendet werden.

Automatisierung und DevOps

In IoT-Lösungen ist die erste Freigabe einer Anwendung der Beginn eines langfristigen Prozesses zum ständigen Verfeinern der Geschäftsvorteile einer IoT-Strategie. Nach der ersten Freigabe einer Anwendung werden die meiste Zeit und der meiste Aufwand darauf verwendet, neue Funktionen zu der aktuellen IoT-Lösung hinzuzufügen. Unter der Prämisse, die Agilität über den gesamten Lebenszyklus der Lösung aufrechtzuerhalten, sollten Sie Services danach bewerten, ob sie eine schnelle Entwicklung und Bereitstellung erlauben, wenn sich die geschäftlichen Anforderungen ändern. Im Gegensatz zu traditionellen Web-Architekturen, bei denen DevOps-Technologien nur die Backend-Server betreffen, erfordert eine IoT-Anwendung auch die Möglichkeit zur schrittweisen Einführung von Änderungen bei verteilten, global verbundenen Geräten. Mit der AWS-Plattform kann ein Unternehmen serverseitige und geräteseitige DevOps-Praktiken zur Automatisierung von Operationen implementieren.

In der AWS-Cloud-Plattform bereitgestellte Anwendungen können mehrere DevOps-Technologien auf AWS nutzen. Um einen Überblick über AWS DevOps zu erhalten, empfehlen wir Ihnen, das Dokument *Einführung in DevOps auf AWS* [1] zu lesen. Obwohl sich die meisten Lösungen bei der Bereitstellung und den Operationsanforderungen unterscheiden, können IoT-Lösungen AWS CloudFormation nutzen, um ihre serverseitige Infrastruktur als Code zu definieren. Als Code behandelte Infrastruktur hat den Vorteil, reproduzierbar, prüfbar und in anderen AWS-Regionen leichter bereitstellbar zu sein. Unternehmen und Organisationen, die AWS CloudFormation zusätzlich zu anderen DevOps-Tools nutzen, erhöhen erheblich ihre Agilität und die Geschwindigkeit, mit der Anwendungsänderungen implementiert werden können.

Um eine IoT-Lösung zu entwickeln, bei der die Grundsätze von Sicherheit und Agilität eingehalten werden, müssen Organisationen auch ihre verbundenen Geräte aktualisieren, nachdem sie in der Umgebung bereitgestellt worden sind. Firmware-Updates bieten für die Unternehmen einen Mechanismus, um neue Funktionen zu einem Gerät hinzuzufügen. Sie sind auch ein wichtiger Pfad zur Bereitstellung von Sicherheits-Patches während der Lebensdauer eines Gerätes. Zum Implementieren von Firmware-Updates in verbundenen Geräten sollte eine IoT-Lösung die Firmware zuerst in einem global zugänglichen Service speichern, z. B. Amazon Simple Storage Service (Amazon S3), um eine sichere, dauerhafte und hoch skalierbare Cloud-Speicherung zu gewährleisten. Anschließend kann die IoT-Lösung Amazon CloudFront implementieren, einen globalen Content Delivery Network- (CDN, Netzwerk zur Bereitstellung von Inhalten) Service, um die in Amazon S3 gespeicherte Firmware zu den Präsenzpunkten mit geringerer Latenz für die verbundenen Geräte zu bringen. Zuletzt können Sie den AWS IoT-Shadow nutzen, um einen Push-Befehl an ein Gerät zu senden, damit die neue Version einer Firmware von einer vorsignierten Amazon CloudFront-URL heruntergeladen wird, die den Zugriff auf die Firmware-Objekte beschränkt, die über das CDN verfügbar sind. Wenn das Upgrade abgeschlossen ist, sollte das Gerät den Erfolg bestätigen, indem es eine Meldung an die IoT-Lösung zurücksendet. Durch die Orchestrierung dieser kleinen Reihe von Services für Firmware-Aktualisierungen können Sie Ihren DevOps-Ansatz für die Geräte kontrollieren und ihn so skalieren, dass er an die IoT-Gesamtstrategie angepasst ist.

Im IoT gehen Automatisierungs- und DevOps-Verfahren über die Anwendungsservices hinaus, die auf der AWS-Plattform bereitgestellt sind, und schließen die verbundenen Geräte ein, die im Rahmen der IoT-Gesamtarchitektur bereitgestellt worden sind. Durch den Aufbau eines Systems, bei dem regelmäßige und globale Aktualisierungen bei Software- und Firmware-Änderungen leicht durchgeführt werden können, können Organisationen den Wert ihrer IoT-Lösung schrittweise erhöhen und diese kontinuierlich erneuern, wenn neue Möglichkeiten auf dem Markt entstehen.

Verwaltung und Sicherheit

Sicherheit ist beim IoT mehr als nur Datenanonymisierung; sie ist die Möglichkeit, Sichtbarkeit, Auditierbarkeit und Kontrolle in einem System bereitzustellen. IoT-Sicherheit beinhaltet die Möglichkeit, Ereignisse im gesamten System zu überwachen und auf diese Ereignisse zu reagieren, um die gewünschte Compliance und Kontrolle zu erreichen. Sicherheit hat bei AWS höchste Priorität. Durch das AWS-Modell übergreifender Verantwortlichkeit verfügt eine Organisation über die Flexibilität, Agilität und Kontrolle, um ihre Sicherheitsanforderungen zu implementieren.[2] AWS verwaltet die Sicherheit **der** Cloud, die Sicherheit **in** der Cloud ist jedoch die Verantwortung des Kunden. Sie behalten die Kontrolle darüber, welche Sicherheitsmechanismen Sie zum Schutz Ihrer Daten, Anwendungen, Geräte, Systeme und Netzwerke implementieren. Darüber hinaus können Unternehmen das umfangreiche Angebot an Sicherheits- und Verwaltungs-Tools nutzen, das AWS und seine Partner bereitstellen, um eine starke, logisch isolierte und sichere IoT-Lösung für eine Flotte von Geräten zu erstellen.

Der erste Service, der zur Überwachung und Sichtbarkeit aktiviert werden sollte, ist AWS CloudTrail. AWS CloudTrail ist ein Web-Service, der Aufrufe von AWS-APIs für ein Konto aufzeichnet und Protokolldateien an Amazon S3 übermittelt. Nach der Aktivierung von AWS CloudTrail sollten Sicherheits- und Kontrollprozesse aufgebaut werden, die auf den Echtzeit-Eingängen von API-Aufrufen basieren, die über ein AWS-Konto erfolgen. AWS CloudTrail bietet eine zusätzliche Ebene von Sichtbarkeit und Flexibilität, indem es eine betriebliche Offenheit in einem System erstellt und iteriert.

Zusätzlich zur Protokollierung von API-Aufrufen sollten Sie Amazon CloudWatch für alle im System genutzten AWS-Services aktivieren. Amazon CloudWatch erlaubt es den Anwendungen, AWS-Metriken zu überwachen sowie benutzerdefinierte Metriken zu erstellen, die von einer Anwendung generiert werden. Diese Metriken können dann bei bestimmten Ereignissen Alarme auslösen. Außer den Amazon CloudWatch-Metriken gibt es auch Amazon CloudWatch Logs, das zusätzliche Protokolle von AWS-Services oder Kundenanwendungen speichert und dann aufgrund dieser zusätzlichen Metriken Ereignisse auslösen kann. AWS-Services, z. B. AWS IoT, werden direkt in Amazon CloudWatch Logs integriert. Diese Protokolle können dynamisch als Datenstrom gelesen und mithilfe von Geschäftslogik und dem Kontext des Systems auf Echtzeit-Anomalien oder Sicherheitsbedrohungen untersucht werden.

Durch die Kombination von Services wie Amazon CloudWatch und Amazon CloudTrail mit den Funktionen der AWS IoT-Identitäten und -Richtlinien kann ein Unternehmen sofort zu Beginn der IoT-Strategie wertvolle Daten zu Sicherheitspraktiken sammeln und Sicherheitsfunktionen proaktiv und befarfsgerecht in seine IoT-Lösung implementieren.

Zusammenbringen von Services und Lösungen

Um die Nutzungsgewohnheiten der Kunden besser zu verstehen, zukünftige Trends vorauszusagen oder eine IoT-Flotte effizienter zu betreiben, muss eine Organisation nicht nur mit einer großen Flotte von *Dingen* in Verbindung bleiben und diese verwalten, sondern auch die potenziell riesige Menge an Daten verarbeiten, die von den verbundenen Geräten gesammelt werden.

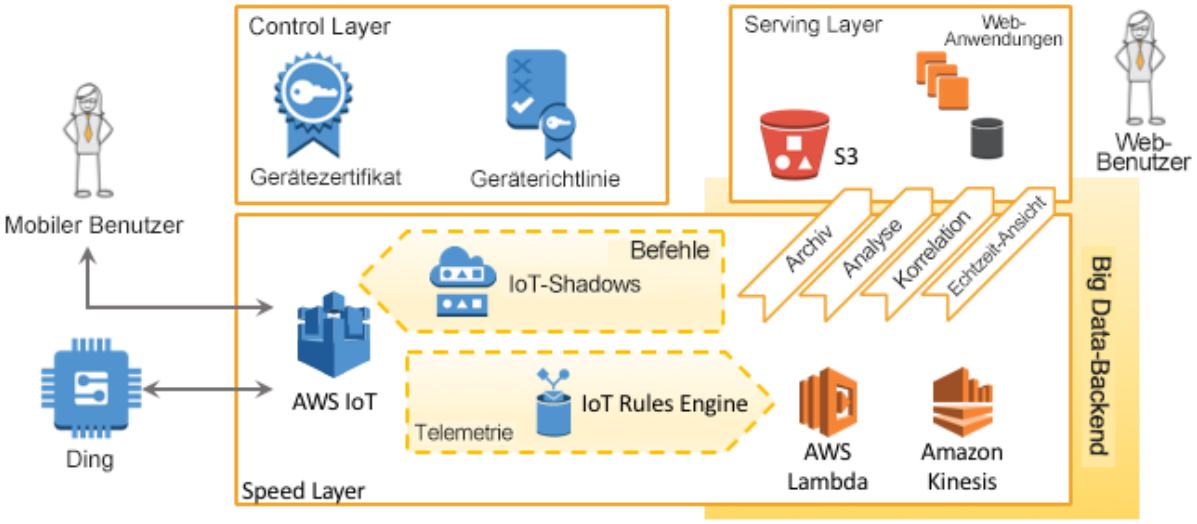
AWS bietet eine Vielzahl von Services zum Sammeln und Analysieren großvolumiger Datensätze an, die oft als Big Data bezeichnet werden. Diese Services können fest in eine IoT-Lösung integriert sein, um die Erfassung, Verarbeitung und Analyse der Daten dieser Lösung zu unterstützen und Hypothesen zu beweisen oder zu widerlegen, die auf IoT-Daten basieren. Die Möglichkeit, mit derselben Plattform Fragen zu formulieren und zu beantworten, die zur Verwaltung einer Flotte von *Dingen* verwendet wird, gibt einer Organisation letztendlich die Möglichkeit, undifferenzierten Aufwand zu vermeiden und geschäftliche Innovationen auf agile Art zu nutzen.

Die hochwertige, zusammenhängende Architekturperspektive einer IoT-Lösung, die IoT, Big Data und andere Services zusammenbringt, wird als Pragma-Architektur bezeichnet. Die Pragma-Architektur ist aus Lösungsschichten zusammengesetzt:

- Things – das Gerät und die Flotte von Geräten
- Control Layer – der Kontrollpunkt zum Zugriff auf den Speed Layer und das Bindeglied für das Flottenmanagement
- Speed Layer – der Gerätetelemetrie-Datenbus mit hoher Bandbreite für eingehende Verbindungen und der Geräte-Befehlsbus für ausgehende Verbindungen

- Serving Layer – der Zugriffspunkt für Systeme und Personen, um mit den Geräten in einer Flotte zu interagieren, um Analysen oder Archivierungen durchzuführen, Daten abzugleichen und Echtzeit-Ansichten der Flotte anzuzeigen.

Pragma-Architektur



Die Pragma-Architektur ist eine einzige zusammenhängende Perspektive, wie die IoT-Grundsätze sich bei der Nutzung von AWS-Services als IoT-Lösung manifestieren.

Ein Szenario einer Pragma-Architektur, die auf einer IoT-Lösung basiert, ist die Verarbeitung von Daten, die von Geräten gesendet werden. Diese Daten werden auch als Telemetrie bezeichnet. Im obigen Diagramm sendet das Gerät regelmäßig Telemetriedaten an das AWS IoT-Device Gateway im Speed Layer, nachdem es sich mit einem Gerätezertifikat authentifiziert hat, das über den AWS IoT-Service im Control Layer vergeben wurde. Die Telemetriedaten werden dann von der IoT Rules Engine als Ereignis verarbeitet, das von Amazon Kinesis oder AWS Lambda für die Nutzung durch Webanwender ausgegeben wird, die mit dem Serving Layer interagieren.

Ein weiteres Szenario einer Pragma-Architektur, die auf einer IoT-Lösung basiert, ist das Senden eines Befehls an ein Gerät. Im obigen Diagramm würde die Anwendung des Benutzers den gewünschten Befehlswert an den IoT-Shadow des Zielgeräts schreiben. Der AWS IoT-Shadow und das Device Gateway arbeiten dann zusammen, um ein intermittierendes Netzwerk zu umgehen und den Befehl an das jeweilige Gerät zu senden.

Dies sind nur zwei geräteorientierte Szenarios aus einer Vielzahl von Lösungen, die mit der Pragma-Architektur möglich sind. Keines dieser Szenarios behandelt die Notwendigkeit, eine möglicherweise riesige Datenmenge zu verarbeiten, die von den verbundenen Geräten gesammelt wird. Daher ist es wichtig, ein integriertes Big Data-Backend zu haben. Das Big Data-Backend in diesem Diagramm ist mit dem gesamten Ökosystem von Echtzeit- und Stapelmodus-Big Data-Lösungen kongruent, die die Kunden bereits mit der zu erstellenden AWS-Plattform nutzen. Einfach ausgedrückt, entspricht aus der Big Data-Perspektive die IoT-Telemetrie den „übernommenen Daten“ in Big Data-Lösungen. Weitere Informationen über Big Data-Lösungen auf AWS finden Sie unter dem unten stehenden Link.

Es gibt eine bunte Palette an Big Data-Lösungen, die Unternehmen bereits mit der AWS-Plattform erstellt haben. Die Pragma-Architektur zeigt, dass durch den Aufbau einer IoT-Lösung auf derselben Plattform das gesamte Ökosystem von Big Data-Lösungen verfügbar ist.

Zusammenfassung

Das Definieren Ihrer Internet of Things-Strategie kann eine wahrhaft transformatorische Aufgabe sein, durch die sich einmalige geschäftliche Innovationen erschließen lassen. Wenn Organisationen bestrebt sind, ihre eigenen IoT-Innovationen einzurichten, ist es von entscheidender Bedeutung, eine Plattform auszuwählen, die die Grundsätze erfüllt: geschäftliche und technische Agilität, Skalierbarkeit, Kosten und Sicherheit. Die AWS-Plattform erfüllt diese Grundsätze einer IoT-Lösung bei Weitem, indem sie nicht nur IoT-Services bereitstellt, sondern diese Services zusammen mit einer breiten, tiefen und hoch angesehenen Palette an Plattform-Services global anbietet. Diese Übererfüllung bringt auch Freiheiten mit sich, die die Kontrolle Ihres Unternehmens über seine Ziele verstärken und es seinen IoT-Lösungen ermöglichen, schneller zu den Ergebnissen zu iterieren, die durch die IoT-Strategie angestrebt sind.

Als nächste Schritte beim Auswerten von IoT-Plattformen empfehlen wir den unten stehenden Abschnitt *Weitere Informationen*, in dem Sie mehr über AWS IoT, Big Data-Lösungen auf AWS und Fallbeispiele von Kunden auf AWS erfahren können.

Mitwirkende

Dieses Dokument wurde von folgenden Personen verfasst:

- Olawale Oladehin, Solutions Architect, Amazon Web Services
- Brett Francis, Principal Solutions Architect, Amazon Web Services

Weitere Informationen

Zusätzliche Informationen finden Sie in den folgenden Ressourcen:

- AWS IoT-Service
- Erste Schritte mit AWS IoT
- AWS-Fallbeispiele
- Möglichkeiten zur Analyse von Big Data mit AWS

Anmerkungen

[1] https://do.awsstatic.com/whitepapers/AWS_DevOps.pdf

[2] https://aws.amazon.com/compliance/shared-responsibility-model/