bbv
MAKING VISIONS WORK.

BOOKLET

IOT-CLOUD-PLATTFORMEN: ENTSCHEIDUNGSHILFE FÜR DIE WAHL DES RICHTIGEN ANBIETERS

inkl. Checkliste für den Betrieb

PROFITIEREN SIE VON UNSERER ERFAHRUNG!

Kontakt Schweiz
bbv Software Services AG
Blumenrain 10
6002 Luzern
Telefon: +41 41 429 01 11
E-Mail: info@bbv.ch

Kontakt Deutschland
bbv Software Services GmbH
Elsenheimerstr. 9
80687 München, Deutschland
Telefon: +49 89 452 4383-0
E-Mail: info@bbv.eu

INHALT

1 VORWORT

Ziel dieses Booklets ist es, Verantwortlichen von IoT-Vorhaben zu Beginn des Projekts bzw. der Produktentwicklung eine Hilfestellung zu bieten. Zielpublikum sind sowohl technische (Entwicklungsleiter, Architekten) als auch nichttechnische Entscheidungsträger (Business Analysten, Projektleiter, Innovationsmanager). Der Fokus des Booklets liegt vor allem auf denjenigen Themen, die bei der Auswahl der Plattform oder generell zu Beginn des IoT-Vorhabens häufig vernachlässigt werden.

Die Kapitel sind jeweils in einen Textteil und eine Checkliste unterteilt. Im Text werden die einzelnen Themen erläutert und Problemfelder aufgezeigt. Die Inhalte wurden aus mehreren IoT-Projekten gesammelt, dazu werden bewährte Best Practices aufgezeigt.

Die Checklisten sind deutlich konkreter und technischer und gehen häufig über den Text hinaus. Sie sind aus einer Sammlung von Fragestellungen aus der Praxis entstanden. Die Idee ist, dass der Leser durch das Ausfüllen der Checklisten pro Plattform einen ganzheitlichen Überblick gewinnt.

Um die Checklisten als Evaluationswerkzeug zu benutzen, können bestimmte Fragen als «Muss-Kriterien» definiert werden. Dies ermöglicht es, das Feld der Plattformen zu lichten. Um die verbleibenden Plattformen bewerten zu können und damit vergleichbar zu machen, muss der Katalog durch eigene, projektspezifische Fragestellungen ergänzt und eine Gewichtung der Fragen eingeführt werden.

bbv bietet basierend auf den Themen in diesem Booklet einen Workshop für die Erarbeitung der Rahmenbedingungen und nicht funktionalen Anforderungen von IoT-Projekten sowie der Grundlagen für den Plattform-Entscheid an. Auch wenn der Plattform-Entscheid bereits gefallen ist, bietet Ihnen der Workshop einen Mehrwert: Der Output dient dann als Grundlage für die Erarbeitung der System-Architektur.

2 EINLEITUNG

Der Markt an IoT-Cloud-Plattformen ist komplex und unübersichtlich. Je nach Quelle ist die Rede von 300 bis 500 unterschiedlichen Anbietern, Tendenz steigend (Stand: 2018). Selbst für Experten ist es nicht möglich, alle Plattformen in der Tiefe zu evaluieren.

Um dennoch zu einem fundierten Entscheid zu kommen, hilft es, die spezifischen Anforderungen des eigenen Projekts aufzulisten und abzuwägen. Dieser Leitfaden soll dabei als Entscheidungshilfe dienen.

3 WELCHE ARTEN VON IOT-CLOUD-PLATTFORMEN GIBT ES?

Grundsätzlich lassen sich IoT-Cloud-Plattformen in zwei Arten unterteilen: Solche, die als Software-as-a-service (SaaS) angeboten werden, und solche, die als Platform-as-a-service (PaaS) angeboten werden.

3.1 SOFTWARE-AS-A-SERVICE (SAAS)-IOT-CLOUD-PLATTFORMEN

SaaS-Angebote bieten fertige IoT-Lösungen out-of-the-box an. Es müssen «nur» noch die Devices angebunden und die Benutzer sowie deren Rechte eingerichtet werden. Die SaaS-Lösungen decken gängige IoT-Use-Cases ab, wie beispielsweise Visualisierung von Sensordaten über die Zeit.

Die SaaS-IoT-Landschaft ist stark fragmentiert und geprägt von Nischenplayern und Start-ups. Ein Teil der SaaS-IoT-Plattformen läuft im Hintergrund auf einer PaaS- oder IaaS-Plattform eines grossen Cloud-Anbieters wie Amazon oder Microsoft. Vor allem kleinere und spezialisierte IoT-Plattformen werden als SaaS-Lösungen angeboten, aber auch einige grosse.

Bei den SaaS-IoT-Plattformen gilt es wiederum die mandantenfähigen SaaS-Plattformen von den dedizierten Lösungen zu unterscheiden:

Mandantenfähige Lösungen laufen auf einer geteilten Infrastruktur. Kein «Mandant» besitzt eine eigene Instanz, sondern alle Mandanten sind auf dem Gesamtsystem konfiguriert. Der Vorteil von Mandantenfähigkeit ist, dass von Economies of Scale profitiert werden kann, was mit zunehmender Anzahl Mandanten die Kosten pro Benutzer bzw. pro Gerät massiv reduziert.

Zudem können Anbieter von mandantenfähigen Lösungen den gesamten Markt abdecken, von kleinen Kunden mit zehn Geräten bis zu Kunden mit einer Million Geräten. Ein Beispiel einer solchen mandantenfähigen SaaS-Lösung ist Azure IoT Central, das IoT-SaaS-Angebot von Microsoft.

Dedizierte SaaS-Lösungen sind häufig versteckte Box-Produkte, wie wir sie aus der Vergangenheit kennen. Sie werden zwar vom Anbieter für den Kunden betrieben, aber auf einer dedizierten Infrastruktur. Mandantenfähigkeit bei solchen dedizierten Systemen heisst dann, dass ein Kunde auf seinem dedizierten System mehrere «Untermandanten» für seine Endkunden einrichten kann. Der Hauptvorteil von solchen Lösungen besteht darin, dass die Lösung in der Regel überall betrieben werden kann: Auf irgendeiner Cloud eines Hyperscalers als auch im eigenen Datencenter On-Premise. Der Betriebsaufwand ist jedoch typischerweise sehr gross, da nur beschränkt von den Skaleneffekten profitiert werden kann.

Bei SaaS-Lösungen wie Thingworx von PTC oder Cumulocity IoT von Software AG können Kunden auswählen, ob sie ein Mandant oder ein dediziertes Setup wollen, wobei Ersteres vor allem für Demo- und Testzwecke oder kleinere Kunden angeboten wird.

Insgesamt liegt der Hauptvorteil von SaaS-Lösungen gegenüber PaaS-Lösungen bei der schnelleren Time-to-Market bei niedrigen Investitionskosten. Der Hauptnachteil: Die möglichen Anwendungsfälle sind vordefiniert, und es ist praktisch nicht möglich, sich mittels eigener Innovationen von der Konkurrenz abzuheben. Zudem ist bei SaaS-Plattformen die Abhängigkeit vom Anbieter (Vendor-Lock-in) am grössten.

3.2 PLATFORM-AS-A-SERVICE (PAAS)-IOT-CLOUD-PLATTFORMEN

PaaS-Plattformen sind im Vergleich zu SaaS keine Ready-out-of-the-Box-Lösungen: Der Cloud-Anbieter liefert einen Baukasten an Diensten (Cloud-Services), aber keine fertige Implementierung. Mit Hilfe dieses Baukastens kann nun die eigene IoT-Cloud-Lösung entwickelt werden, inklusive der eigenen, spezifischen Anwendungsfälle oder der Integrationen in Drittsysteme. Die PaaS-Lösungen finden sich praktisch ausschliesslich bei den grossen Cloud-Anbietern, namentlich Microsoft Azure, AWS, IBM und Google.

Azure und AWS als führende Anbieter im PaaS-Bereich bieten heute je weit über hundert PaaS-Dienste an. Das geht von Datenbank- und Big-Data-Lösungen über IoT-spezifische Dienste, Entwicklerwerkzeuge, Identity- und Access-Management, Web- und Mobile-Dienste, Container-Lösungen, Dienste für Sicherheit bis hin zu Integrationslösungen in diverse Drittsysteme. All diese Dienste sind «Managed Services», werden also vom Cloud-Anbieter betrieben, und der Cloud-Anbieter ist verantwortlich für die Verfügbarkeit, Skalierbarkeit und Sicherheit dieser Dienste.

Der Hauptvorteil von PaaS-Lösungen liegt darin, dass die eigene Lösung auf bewährten, sicheren und skalierbaren Services aufsetzen kann und die Plattform dennoch genug Freiheiten bietet, um eigene, spezifische Anwendungsfälle und Innovationen umzusetzen. Hauptnachteile gegenüber SaaS sind eine weniger schnelle Time-to-Market und höhere Entwicklungskosten.

3.3 HYBRIDE FORMEN ZWISCHEN SAAS UND PAAS

Die Unterteilung in SaaS- oder PaaS-Plattformen ist nicht immer einfach. So kann etwa SAP Leonardo nicht eindeutig einer Kategorie zugeordnet werden. Zudem gibt es Anbieter wie Microsoft, die sowohl eine PaaS-Lösung (Azure IoT) als auch eine SaaS-Lösung (Azure IoT Central) anbieten.

Neben SaaS- und PaaS-Lösungen gibt es noch den IaaS-Lösungsansatz sowie IoT-Dienstleistungen. Auf diese beiden Formen wird in diesem Booklet später nicht mehr genauer eingegangen.

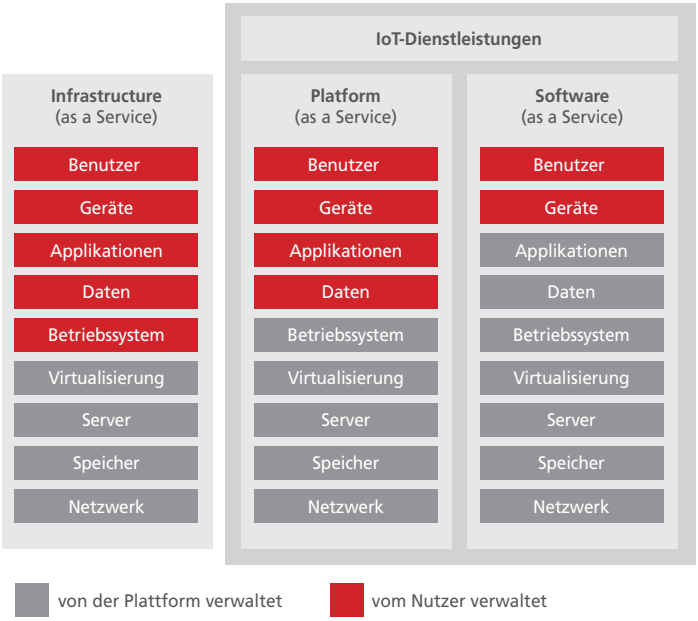
3.4 INFRASTRUCTURE-AS-A-SERVICE (IAAS)

Infrastructure-as-a-Service bedeutet, dass man von einem Cloud-Provider nur virtuelle Server mietet. Der Cloud-Provider ist verantwortlich für die Verfügbarkeit der virtuellen Maschinen sowie des Netzwerks, in welches die Server eingebunden sind. Der Cloud-Provider ist aber nicht verantwortlich für Software, die auf diesen Servern läuft oder für die Datenspeicherung auf diesen Servern. Daher gibt es keine IaaS-IoT-Plattform – der Kunde müsste den gesamten IoT-Applikationsstack selbst auf der IaaS-Infrastruktur betreiben.

Allerdings sind hybride Formen von PaaS und IaaS im IoT-Bereich gerade in grossen Firmen häufig anzutreffen. Diese Unternehmen wollen für die Konnektivität und Kommunikation zu den Devices einen PaaS-Service nutzen (etwa den Azure IoT Hub oder den Amazon Device Gateway), da diese Dienste bereits alle funktionalen und nicht funktionalen Anforderungen abdecken, wie Sicherheit, Verfügbarkeit, Skalierbarkeit, Compliance. Für die Verarbeitung der IoT-Daten soll dann aber ein spezifisches Big-Data-Tool genutzt werden, welches als PaaS-Service nicht exis-

tiert. Dieses Tool kann auf dem eigenen IaaS-Cluster installiert und betrieben werden. Diese Variante ist deshalb so beliebt, weil es im Big-Data-Bereich Dutzende spezialisierter Tools gibt.

Ein anderer Grund für eine PaaS/IaaS-Hybrid-Lösung kann die Reduktion der Abhängigkeit vom Cloud-Anbieter sein: Je weniger PaaS-Services man nutzt, desto kleiner ist der Vendor-Lock-in. Gleichzeitig steigen bei IaaS aber die Entwicklungskosten sowie in der Regel auch die Betriebskosten, da einerseits nicht mehr im selben Ausmass von Skaleneffekten (Economies of Scale) profitiert werden kann und andererseits bei IaaS ein grosser Teil des Applikationsstacks selbst betrieben werden muss.



Übersicht über die verschiedenen Arten der IoT-Cloud-Plattformen

3.5 IOT-DIENSTLEISTUNGEN

Es gibt einige Unternehmen, die Dienstleistungen rund um bestehende IoT-Plattformen aufgebaut haben und diese ihren Kunden als Paket verkaufen. Dieses Paket aus bestehender PaaS/SaaS-Plattform und Dienstleistungskatalog wird dann als eigene IoT-Plattform vermarktet, obschon es sich eigentlich nicht um eine neue Plattform handelt.

Solche Paketlösungen haben den Vorteil, dass etwa die Time-to-Market von PaaS-Lösungen verringert werden kann, da der Dienstleister bereits viel Know-how und zum Teil auch schon fertige Software-Module etwa für Routine-Aufgaben mitbringt.

Gewisse Dienstleister bieten rund um die IoT-Lösung einen Managed Service an, sie kümmern sich also auch um den späteren Betrieb der Lösung, den Support, die Wartung, die Einhaltung eines allfälligen SLA und die Abrechnung (Billing). Gerade bei PaaS-Lösungen ist das ein grosser Vorteil für ein Unternehmen ohne internes Know-how in diesen Bereichen. Nachteilig wirkt sich hier aus, dass sich der Kunde nicht nur in die Abhängigkeit eines Cloud-Anbieters, sondern zusätzlich eines Dienstleisters begibt – technisch, wirtschaftlich und auch rechtlich. Solche Partnerschaften müssen daher sehr gut geprüft werden.

4 TIME-TO-MARKET UND LANGFRISTIGE VISION

IoT-Projekte beginnen in der Regel mit einem MVP, einem Minimum Viable Product, manchmal auch Pilot genannt. Ein MVP ist eine Version eines neuen Produkts, das mit dem geringstmöglichen Aufwand erstellt wird, um für die Validierung mit Kunden verwendet zu werden. Häufig werden diese MVPs innerhalb weniger Wochen oder Monate entwickelt und dann an einer Branchenmesse präsentiert. Damit können Unternehmen bereits in einer frühen Phase prüfen, ob es eine Nachfrage nach der IoT-Lösung gibt und die Anwendungsfälle sowie das Business-Modell für eine allfällige Weiterentwicklung schärfen.

Schnell sein, im Sinne einer kurzen Time-to-Market, ist einer der Schlüssel zum Erfolg. Damit man aber nach dem MVP nicht in einer Sackgasse landet, muss bei der Wahl der Plattform darauf geachtet werden, dass die Plattform die Skalierbarkeit gewährleisten kann bzw. bei grosser Skalierung wirtschaftlich bleibt und dass sich auch komplexere Use Cases umsetzen lassen – beispielsweise eine sichere Remote-Update-Funktionalität oder eine komplexe Mandantenfähigkeit (mehr zu Mandantenfähigkeit folgt).

Ein anderer Ansatz ist es, für das MVP/den Piloten eine Plattform zu wählen und diese Wahl später nochmals zu revidieren und auf einer anderen Plattform neu zu beginnen. Während solche, bewusst geplanten, Umwege in der klassischen Softwareentwicklung selten sind, kommen sie bei der Entwicklung von Cloud-Applikationen verhältnismässig häufig vor: Dank der Flexibilität der Cloud können auch komplexe Systeme schnell heruntergefahren oder hochgezogen werden, ganz ohne Investitionskosten in Hardware oder in Softwarelizenzen. Allerdings ist bei einem Neustart zu beachten, die allenfalls bereits geweckten Erwartungen der Kunden nicht zu enttäuschen.

Folgende Fragen helfen Ihnen bei der Wahl des richtigen IoT-Cloud-Anbieters in diesem Bereich. Prüfen Sie bei jeder Frage, wie wichtig sie für Ihr Projekt ist (Relevanz) und wie gut der Anbieter diesen Punkt erfüllt (Erfüllungsgrad).

Tabelle 1

	Relevanz	Erfüllungs-grad
Time-to-Market: Wie schnell kann mein MVP auf der Plattform umgesetzt werden?		
Entwicklungskosten: Was kostet mich die Umsetzung des MVPs?		
Kann die Plattform jederzeit auf mein maximales Mengengerüst hochskalieren?		
Wie hoch sind die Betriebskosten bei voller Skalierung? Kommt dann mein Business Case bei diesen Kosten noch zustande?		
Zukunftssicherheit: Beinhaltet meine langfristige Produktvision auch Cross-Cutting Concerns, die das MVP nicht hat, z. B.: Mandantenfähigkeit, Benutzer- und Rechteverwaltung, Audit, Monitoring, Support-Prozesse, nicht-funktionale Anforderungen? Können auch diese zukünftigen Prozesse abgebildet werden?		

5 FUNKTIONALITÄT & INNOVATION

Für die Evaluation einer IoT-Plattform ist zunächst der angebotene Funktionsumfang entscheidend. In erster Linie sollten die eigene Vision und sämtliche davon abgeleiteten Anwendungsfälle auf der Plattform abgebildet werden können. Dabei muss geprüft werden, wie stark die Plattform die weitere Entwicklung unterstützt beziehungsweise einschränkt. Dies ist insbesondere bei den SaaS-Plattformen häufig schwierig abzuschätzen.

Es geht aber gleichzeitig auch darum, keine Trends und Innovationen im IoT-Bereich zu verpassen. Das Internet der Dinge ist immer noch stark geprägt von Innovationen einzelner Anbieter, Standardisierungsbemühungen stehen noch ganz am Anfang. In diesem Umfeld ist es wichtig, auf einen Anbieter zu setzen, der bei der Entwicklung des Internets der Dinge vorne mit dabei ist und in der Lage ist, mit den Entwicklungen Schritt zu halten, wenn nicht sogar diese Entwicklungen zu prägen.

Während die grossen Anbieter mit dem Angebot sehr stark in die Breite gehen (weit über 100 Cloud-Services bei Amazon und Microsoft), sind es die kleinen Anbieter, die in der Tiefe den Unterschied ausmachen können. So gibt es einige kleinere Plattformen, die sich dank branchenspezifischer, regionaler oder technologiespezifischer Ausrichtung gegen die Grossen erfolgreich zur Wehr setzen.

Folgende Fragen helfen Ihnen bei der Wahl des richtigen IoT-Cloud-Anbieters in diesem Bereich. Prüfen Sie bei jeder Frage, wie wichtig sie für Ihr Projekt ist (Relevanz) und wie gut der Anbieter diesen Punkt erfüllt (Erfüllungsgrad).

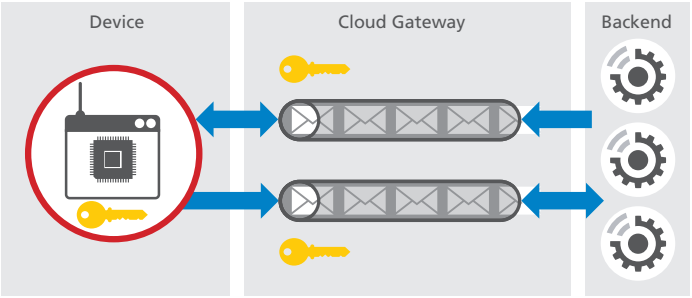
Tabelle 2

	Relevanz	Erfüllungs-grad
Können sämtliche geplanten Anwendungsfälle abgebildet werden?		
Wie gross ist der Funktionsumfang der Cloud-Plattform? Wie viele relevante Services bietet die Plattform out-of-the-box?		
Welche Einschränkungen gibt es und wie gut kann man damit leben?		
Wie stark engagiert sich der Anbieter in Standardisierungsgremien?		
Wie schnell adaptiert der Anbieter neue Trends und Entwicklungen?		
Benötigt man einen speziellen Technologie-Stack und unterstützt der Anbieter diesen Stack?		
Wie gut ist der Anbieter auf die spezifischen Anwendungsfälle/Anforderungen meiner Branche ausgerichtet?		

6 KONNEKTIVITÄT

Bei der Konnektivität unterscheiden sich die technischen Lösungen deutlich. Es gibt IoT-Plattform-Anbieter, welche auf VPN-Lösungen setzen, andere benötigen eine offene HTTPS-Schnittstelle auf dem Device, wieder andere setzen auf FTP oder proprietäre Protokolle. Es kann sein, dass solche Lösungen skalierbar, sicher und hoch verfügbar sind, aber sie sind es nicht «by Design».

Wenn man sich das Konnektivitätskonzept von bekannten IoT-Plattformen wie AWS, Azure oder Google Cloud anschaut, sieht man, dass sich ein bestimmtes Design für die Konnektivität im IoT-Bereich etabliert: Alle diese Plattformen bieten in der Cloud einen Service an, welcher in beide Richtungen (bidirektional) mit den Devices kommuniziert. Diese Dienste funktionieren, stark vereinfacht ausgedrückt, folgendermassen: Wenn das Device der Cloud eine Nachricht sendet, stellt dieser Dienst die Nachricht in eine Message-Queue, die vom Backend konsumiert wird. Wenn das Cloud-Backend dem Device etwas senden will, wird die Nachricht in eine andere Message-Queue gestellt. Ist das Device online, holt es sich die Nachricht durch seine ausgehende Verbindung ab. Für den Zugriff auf das Backend verwendet das Device ein eigenes, eindeutiges Zertifikat, welches nur Zugriff auf seine Nachrichten erlaubt (siehe Grafik).



Vereinfachtes Schema des Konnektivitätskonzepts von führenden IoT-Plattformen.

Als Standard-Protokoll für die Device-Cloud-Konnektivität scheint sich das MQTT Protokoll zu etablieren. IoT-Cloud-Plattformen sollten dieses Protokoll unterstützen.

Dieses Design hat folgende Vorteile:

- Die Devices sind «by Design» voneinander isoliert, nicht wie beispielsweise bei einer VPN-Lösung, wo man eine Isolierung konfigurieren muss.
- Die Cloud-Dienste können fast beliebig horizontal skalieren und somit mit Millionen von Devices sprechen und Milliarden von Nachrichten pro Tag entgegennehmen. Oder auch ganz günstig mit nur einem Dutzend Devices kommunizieren.
- Das Device muss keine eingehende Verbindung zulassen. Eingehende Netzwerk-Ports auf dem Device können geschlossen werden. Das Device kann hinter Firewalls und Routern stehen. Es muss lediglich eine ausgehende Verbindung öffnen können. Der Angriffsvektor wird dadurch minimiert.
- Die Cloud-Dienste unterstützen mehrere sichere, effiziente, offene und standardisierte Protokolle, etwa AMQP oder MQTT sowie HTTPS.

Folgende Fragen helfen bei der Wahl des richtigen IoT-Cloud-Anbieters in diesem Bereich. Prüfen Sie bei jeder Frage, wie wichtig sie für Ihr Projekt ist (Relevanz) und wie gut der Anbieter diesen Punkt erfüllt (Erfüllungsgrad).

Tabelle 3

	Relevanz	Erfüllungs-grad
Wie sicher ist das Konnektivitätskonzept des Cloud-Anbieters «by Design»? Entspricht es einer modernen IoT-Architektur?		
Wie aufwändig ist die Netzwerkkonfiguration auf der Device-Seite? Müssen eingehende Netzwerk-Ports geöffnet werden? Welche ausgehenden Netzwerk-Ports müssen geöffnet werden? Ist das akzeptabel?		
Werden offene, standardisierte, sichere Protokolle verwendet? Kann das Device mit diesen Protokollen angebunden werden?		
Falls proprietäre Protokolle verwendet werden: Ist die Sicherheit dieser Protokolle gewährleistet/dokumentiert?		
Unterstützt die Plattform MQTT? Können Devices mit einem beliebigen MQTT SDK angebunden werden?		
Stehen Device-seitig SDKs/Libraries für meinen Technologiestack zur Verfügung?		
Wie sieht der Long Term Support (LTS) der Device-SDKs bzw. der Device-Schnittstelle aus?		
Remote-Update-Prozess: Wie schnell können Sicherheitslücken auf dem Device gepatched werden?		
Können sich Devices mittels asymmetrischer Schlüssel/Zertifikate authentifizieren?		

Gibt es die Möglichkeit, Schlüssel und Zertifikate regelmässig auszutauschen (Key-Rollover-Prozess)?		
Gibt es eine Public-Key-Infrastruktur für die Device-Authentisierung und wie ist sie aufgebaut?		
Wird Device-seitig ein sicherer Schlüsselspeicher (TPM, HSM) gebraucht/unterstützt?		
Gibt es ein Konzept für Edge-Computing?		
Welche Anforderungen an die Leistungsfähigkeit des Edge-Devices bestehen seitens der Plattform und können diese erfüllt werden?		
Bietet das Edge-Device ein Plug-in-Modell (z. B. via Docker-Container)?		
Kann das Edge-Device remote aktualisiert werden?		
Können höhere Edge-Technologien eingesetzt werden wie Stream-Analyse und Machine Learning?		

7 DEVICE LIFECYCLE MANAGEMENT

Das Device Lifecycle Management für IoT- bzw. IoT-Edge-Devices kann in folgende Abschnitte unterteilt werden:

- Bezug der Hardware (für Edge-Devices oder Gateways)
- Initiales Device-Setup und Vulnerability Management
- Device Provisioning
- Connectivity-Setup
- Over-the-air-Updates
- Monitoring
- Wiederverkauf
- Deprovisioning / Entsorgung

Entscheidend bei der Auswahl der Cloud-Plattform ist, dass sämtliche nachstehend beschriebenen Prozesse automatisiert werden können, damit die Lösung auch bei vielen Devices skaliert.

Bezug der Hardware

IoT-Devices können über drei Arten mit dem Internet verbunden werden: Direkt, über ein Field-Gateway oder über ein Edge-Device, das als Field-Gateway dient. Ein Field-Gateway kann etwa ein Mobilfunk-Gateway mit SIM-Karte sein oder auch ein Protokoll-Umwandler, das ein Nicht-IP-fähiges Gerät ans Internet anschliesst. Edge-Devices besitzen in der Regel auch Gateway-Funktionalitäten. Darüber hinaus können sie auch Business-Logik lokal ausführen, etwa in Form von Containern, die von der Cloud geladen werden.

Für die Hardware für Field-Gateways oder Edge-Devices muss ein Hersteller evaluiert und eine Lieferkette etabliert werden. Je nach Cloud-Plattform gibt es ein Zertifizierungsprogramm, welches geeignete Hardware in einem Katalog ausweist.

Initiales Device-Setup und Vulnerability Management

Das initiale Device-Setup von Edge-Devices oder Field-Gateways bezieht sich auf die Installation des Betriebssystems und ggf. des Edge-Frameworks. Idealerweise wird das Device bereits vorinstalliert vom Hersteller geliefert, inkl. allenfalls benötigter Lizenzen (etwa für Windows Devices). Eine spezielle Herausforderung ist das Vulnerability Management des Software-Stacks auf Betriebssystem- und Framework-Ebene. Es muss ein Prozess etabliert werden für das schnelle Beurteilen und Patchen von neu bekannt gewordenen Sicherheitslücken, beispielsweise im TLS-Stack von Linux. Allenfalls bietet der Hardware-Lieferant diesen Prozess bereits an, insbesondere für Customized Linux (Yocto).

Auch der Prozess für das Device-Hardening sollte mit dem Hardware-Lieferant besprochen werden. Dabei geht es unter anderem darum sicherzustellen, dass keine unnötigen Dienste auf dem Device laufen und alle Ports geschlossen sind. Auch die Absicherung des physikalischen Zugriffs gehört dazu. Auch das Device-Hardening und entsprechende Test-Suiten sollten automatisiert werden.

Device Provisioning

Beim Device Provisioning geht es um die Frage, wie das Device zu seiner Identität kommt, mit der es sich an der Cloud anmelden kann. Dies ist häufig ein Zertifikat, das auf dem Device installiert wird. Gewisse Plattformen bieten dafür einen Device Provisionierungs-Service an, der es ermöglicht, diesen Ablauf zu automatisieren. Dennoch bleibt ein gewisser Implementierungsaufwand, um die Device-Provisionierung an die eigenen Prozesse und Systeme anzupassen. Entscheidend ist der Zeitpunkt der Provisionierung: Wird das Device bereits vor der Auslieferung an der Cloud angemeldet oder wird es im Feld provisioniert? Bei einer vorgän-

gigen Provisionierung muss damit gerechnet werden, dass das Device über eine längere Zeit nicht mehr mit der Cloud verbunden ist, weil es in ein Lager zurückgeht. Dies kann dazu führen, dass Zertifikate ablaufen, bevor das Device in Betrieb genommen wird. Bei einer Provisionierung im Feld müssen Service-Techniker geschult werden, wie das Device vor Ort zu provisionieren ist.

Wird für die Device-Authentifizierung ein Zertifikat verwendet, muss allenfalls eine eigene Public-Key-Infrastruktur aufgebaut werden.

Neben den Zugangsdaten wird bei der Provisionierung auch die initiale Konfiguration auf das Gerät gespielt. Auch hier sollte die Cloud-Plattform bereits einen Automatisierungsmechanismus anbieten, zum Beispiel mit Vorlagen (Device-Templates), die automatisch auf gewisse Gerätegruppen angewendet werden.

Connectivity-Setup

Grundsätzlich kann jedes IoT-Device (bzw. je Field-Gateway) über drei Arten mit dem Internet verbunden werden: Via lokale Infrastruktur (LAN, WLAN), via eigenen Zugang über Breitband-Mobilfunk oder via LPWAN (Low-Power Wide-Area Network). In Zukunft wird auch der Zugang via Satelliten eine realistische Option sein.

Beim Zugang via Mobilfunk kann die Connectivity idealerweise bereits vor der Auslieferung konfiguriert werden. Die grösste Herausforderung ist das Verwalten der Mobilfunk-Verträge (inkl. Roaming) und der dazugehörigen SIM-Karten bzw. eSIM-fähigen Devices.

Beim Zugang via LAN / WLAN müssen jedem einzelnen Device die

lokalen Netzwerk-Zugangsdaten konfiguriert werden, inkl. allfälliger Proxy- und DNS-Server. Dies ist häufig nicht vorgängig möglich, da nicht bekannt ist, welches Device in welchem lokalen Netzwerk installiert wird. Proxy-Server stellen dabei eine grosse Herausforderung dar, insbesondere wenn sie die TLS-Verbindung zum Cloud-Gateway unterbrechen (TLS Interception).

LPWAN-Verbindungen kommen mit ihren ganz eigenen Herausforderungen und decken ihre eigene Kategorie von IoT-Use-Cases ab.

Over-the-air-Updates

Ist das Device im Feld installiert, konfiguriert und mit der Cloud verbunden, sollte es aus der Cloud aktualisiert werden können. Dies betrifft insbesondere Sicherheitspatches im Software-Stack, aber auch das Einspielen von neuen Server-TLS-Root-Zertifikaten des Cloud-Gateways oder Konfigurations-Updates. Bei Edge-Computing muss die Cloud-Plattform auch ein Lifecycle-Management für Container-Images anbieten, die auf die Devices geladen werden sollen.

Die Update-Funktionalität sollte im Fehlerfall automatisch einen Rollback auf ein funktionierendes Setup machen können. Die Remote-Update-Funktionalität muss auch damit umgehen können, dass gewisse Devices einen sehr alten Software-Stand aufweisen und trotzdem aktualisiert werden können. Weiter muss die Integrität von Software-Updates sichergestellt werden, denn noch schlimmer als Datenverlust wiegt das Risiko, dass IoT-Systeme Malware (Viren, Randsomware, Bitcoin-Mining etc.) im grossen Stil verteilen, nicht nur auf die IoT-Geräte, sondern weiter innerhalb von (Kunden-)Netzwerken.

Monitoring

Monitoring

Während der aktiven Phase der IoT-Geräte sollten diese aus der Cloud heraus überwacht werden können. Man spricht von einem Flottenmonitoring, da sowohl jedes einzelne als auch Gruppen von Devices überwacht werden. Die Überwachung bezieht sich auf den Zustand des Devices, aber auch auf dessen Konfiguration, auf Zustände von Edge-Containern und auf System-Parameter wie die Auslastung oder der Energieverbrauch. Unter Umständen gehört auch ein automatisiertes Scanning auf Malware zum Monitoring der Edge-Devices dazu. Ebenso sollten Tests aus dem Device-Hardening auch im Feld regelmässig durchgeführt werden können (namentlich das Erkennen von unnötigen Diensten und offenen Ports).

Wiederverkauf

Wie ein Auto, das mehrfach den Besitzer wechselt, können auch IoT-fähige Geräte und Maschinen wiederverkauft werden. Dabei stellt sich die Frage, wie mit den Daten des Vorgängers umgegangen wird. Bei einem Autokauf kann ich in der Regel das Service-Buch über die ganze Lebensdauer des Autos einsehen. Zudem sehe ich den Kilometerstand. Aber ich sollte nicht wissen, wo der Vorgänger mit dem Auto überall gewesen ist. Welche Daten darf also ein Käufer eines IoT-Geräts einsehen, wenn er dieses erwirbt? Unterstützt meine Plattform den Anwendungsfall, dass ein IoT-Gerät in seinem Leben den Besitzer (bzw. Mandanten) wechselt?

Verwandt mit der Problemstellung des Wiederverkaufs ist gerade bei IoT-fähigen Maschinen auch die Fragestellung, ob Daten aus den Abnahmetests innerhalb der Produktion bereits dem ersten Käufer zur Verfügung gestellt werden oder nicht. Ebenso ob die Maschine ihre Identität bei einem Verkauf behält (Identität = Seriennummer) oder nicht (Identität = Seriennummer & Besitzer-Id).

Deprovisioning / Entsorgung

Bei der Deprovisionierung muss sichergestellt werden, dass das Device auch in der Cloud abgemeldet wird und somit die Zugangsdaten die auf dem Device gespeichert sind, ungültig werden. Dies ist schwierig, falls die Cloud nur das Root-Zertifikat kennt und alle davon abgeleiteten Zertifikate akzeptiert werden.

Folgende Fragen helfen bei der Wahl des richtigen IoT-Cloud-Anbieters in diesem Bereich. Prüfen Sie bei jeder Frage, wie wichtig sie für Ihr Projekt ist (Relevanz) und wie gut der Anbieter diesen Punkt erfüllt (Erfüllungsgrad).

Tabelle 4

	Relevanz	Erfüllungsgrad
Gibt es ein Zertifizierungsprogramm, welches «Plug-and-Play»-fähige Devices als Katalog auflistet?		
Bietet die Plattform Möglichkeiten zur Entdeckung von Sicherheitslücken im Software-Stack?		
Bietet die Plattform Möglichkeiten zur Entdeckung von Sicherheitslücken in der Konfiguration (z. B. unnötig offene Ports)?		
Wie hoch ist der Automatisierungsaufwand für das Device-Provisioning?		
Unterstützt die Plattform eine PKI für Device-Zertifikate?		
Können Mobilfunk-Verträge / SIMs /eSIMs mit der Plattform verwaltet werden?		

Kann das Edge-Framework mit Proxy-Servern und TLS-Interception umgehen?		
Werden OtA-Updates für Betriebssystem, Applikations-Stack und Konfiguration unterstützt?		
Können Updates «at Scale» durchgeführt werden, also automatisiert für eine bestimmte Gruppe von Devices?		
Können alle wichtigen Parameter der Geräteflotte überwacht werden?		
Kann ein Befall mit Malware auf den IoT-Devices erkannt werden?		
Kann die Integrität von Updates sichergestellt werden?		
Ist der Wiederverkauf / Mandantenwechsel von End-Geräten auf der Plattform vorgesehen?		
Können einzelne Geräte sicher deprovisioniert werden?		

8 SKALIERBARKEIT & BIG DATA

Das Thema Big Data wird häufig in IoT-Projekten unterschätzt. Es gibt IoT-Projekte ohne Big Data und solche mit Big Data. Zu welcher Sorte Ihr Projekt langfristig gehört, muss jedoch zu Beginn geklärt werden.

Wann spricht man von Big Data? Laienhaft ausgedrückt: Solange alle IoT-Daten in einer relationalen Datenbank effizient und kostengünstig gespeichert werden können, ist es kein Big-Data-Projekt. Sobald eine relationale Datenbank aus Performance-, Kosten- oder Speicherkapazitätsgründen nicht mehr effizient ist, müssen Alternativen gefunden werden, etwa nicht-relationale Datenbanken, verteilte Systeme zur Datenverarbeitung oder ein Data Lake. Dieser Big-Data-Bereich beginnt ungefähr ab Datenmengen in Terrabyte-Grösse.

Wie schnell man auf so grosse Datenmengen kommt, zeigt das exemplarische Mengengerüst unten, basierend auf der Anzahl Maschinen, der Anzahl Nachrichten und der Grösse der einzelnen Nachrichten während der Übertragung und beim Speichern. Ob Big Data oder kein Big Data hat einen massiven Einfluss auf die System-Architektur und die Kosten. Falls sich das System im Endausbau im Big-Data-Bereich befindet, muss zwingend eine IoT-Plattform evaluiert werden, die Big-Data-Technologien unterstützt. Während des Projekts ist ein Last Test, um das Mengengerüst sowie die Skalierbarkeit und die Kostenrechnung zu validieren, zwingend.

Es ist durchaus valid, eine reine IoT-Plattform zu evaluieren, welche die Daten nur während 30 Tagen speichert, diese Daten jedoch laufend in ein externes Big-Data-System exportieren kann. So können beispielsweise Azure IoT Central und Cumulocity IoT kein Big Data speichern, bieten aber diesen Export (z. B. in die Azure Data Platform) an.

Nachricht	Typ	Grösse in Bytes im Speicher	Anzahl Nachrichten pro Tag / Device	Kilobytes / Tag / Device
Nachricht X	Event-basiert	50	450	22.5
Nachricht Y	Zeitserie	100	1440	144.0
Nachricht Z	Event-basiert	200	2	0.4
Summe			1892	166.9

Anzahl Devices	100’000		
Gigabytes / Tag	17	Nachrichten / Sek.	2'190
Gigabytes / Monat	501	Nachrichten / Tag	189'200'000
Terrabytes / Jahr	6.1	Nachrichten / Monat	5’676’000’000

Folgende Fragen helfen bei der Wahl des richtigen IoT-Cloud-Anbieters in diesem Bereich. Prüfen Sie bei jeder Frage, wie wichtig sie für Ihr Projekt ist (Relevanz) und wie gut der Anbieter diesen Punkt erfüllt (Erfüllungsgrad).

Tabelle 5

	Relevanz	Erfüllungsgrad
Unterstützt die Plattform «Big Data»?		
Werden die für mein Projekt relevanten Big-Data-Technologiestacks von der Plattform unterstützt?		
Sind die unterstützten Tools standardisiert und open source oder proprietär?		
Wird meine bevorzugte Big-Data-Architektur von der Plattform unterstützt (z. B. Lambda-Architektur, MPP-Systeme, ETL-/ELT-Pipelines, nicht-relationale Datenbanken, Data-Lake-Systeme)?		
Verwaltet der Cloud-Provider die Big-Data-Systeme oder muss man das selbst machen (IaaS vs. Managed Cluster vs. Managed Service)?		
Wie einfach können Machine-Learning-Modelle trainiert und deployed werden?		
Welche SDKs für die Verarbeitung von Big Data stehen bereit? Wie einfach können Daten kontinuierlich in einem offenen Format exportiert werden? In welche Big Data Systeme können Daten laufend exportiert werden (Out-of-the-Box)?		

9 VERFÜGBARKEIT, BACKUP & VERANTWORTLICHKEITEN

Neben der im SLA zugesicherten theoretischen Verfügbarkeit der Cloud-Plattform (siehe Kapitel «Vertrag und SLA») ist auch wichtig zu wissen, was der Cloud-Anbieter im Detail für konkrete Massnahmen und Prozesse hat, um diese Verfügbarkeit sicherzustellen und welche Verantwortung dem Kunden (also Ihnen) zukommt. Es kann beispielsweise sein, dass der Cloud-Anbieter eine hohe Verfügbarkeit gewährleistet, aber nur, wenn die eigene Lösung über mehrere Datencenter gespiegelt wird. Dies einzurichten liegt dann in Ihrer Verantwortung.

Verlassen Sie sich auch nicht nur auf die Backup- und Business-Continuity-Pläne des Cloud-Anbieters, sondern erstellen Sie Ihre eigenen entsprechenden Prozesse und testen Sie diese auch regelmässig.

Folgende Fragen helfen bei der Wahl des richtigen IoT-Cloud-Anbieters in diesem Bereich. Prüfen Sie bei jeder Frage, wie wichtig sie für Ihr Projekt ist (Relevanz) und wie gut der Anbieter diesen Punkt erfüllt (Erfüllungsgrad).

Tabelle 6

	Relevanz	Erfüllungsgrad
Ist die zugesicherte Verfügbarkeit akzeptabel und ist dokumentiert, ob der Anbieter diese Verfügbarkeit in der Vergangenheit einhalten konnte?		
Bietet der Anbieter automatisches Backup an?		
Bietet der Anbieter Replizierung und Failover an?		
Gibt es einen Desaster-Recovery-Plan des Anbieters?		
Sind die Verantwortlichkeiten zwischen Anbieter und mir als Kunden in all diesen Bereichen klar geregelt?		
Sind bezüglich dieser Massnahmen die Auswirkungen auf die Kosten klar?		

10 ERWEITERBARKEIT, INTEGRATION UND MANDANTENFÄHIGKEIT

Die Erweiterbarkeit ist entscheidend für die Wahl zwischen PaaS- und SaaS-Lösung, wird aber auch schnell komplex. Dazu ein Beispiel: IoT-Lösungen müssen häufig mandantenfähig sein, so darf Kunde A seine Maschinen sehen, aber nur seine und nicht diejenigen von Kunde B. So weit, so gut: Eine solche einfache Isolierung der einzelnen Mandanten mit ihren Devices können auch SaaS-Plattformen umsetzen. Die Welt ist aber häufig komplizierter als das, zum Beispiel für Service-Partner. Service-Partner X sollte Devices von Kunde A und B sehen dürfen, aber nur diejenigen, bei denen er auch Service-Partner ist. Wenn dann beispielsweise noch ein Franchise-System dazukommt, kann man sich leicht vorstellen, dass solche Anforderungen nicht zur Standardfunktionalität von SaaS-IoT-Plattformen gehören. Eine andere Anforderung, mit der sich die meisten Plattformen erstaunlich schwertun, ist die Aggregation der IoT-Daten von Devices in unterschiedlichen Zeitzonen. Auf PaaS können solche Anforderungen umgesetzt werden.

Bei der Integration sieht es häufig ähnlich aus: Der Standardanwendungsfall von SaaS-IoT-Plattformen ist die Datenvisualisierung für Benutzer mit Hilfe von Charts, Reports und Dashboards. Im Rahmen der Digitalisierung will man aber eigentlich das Gegenteil: automatisieren. Die Daten, die man von den Devices erhält, sollen zu Informationen verdichtet und diese Informationen wieder anderen Systemen zur Verfügung gestellt werden. Integrationsmöglichkeiten in Umsysteme sind notwendig wie beispielsweise ERP, MES, CRM, PIM, DWH, Lagerverwaltung sowie Überwachungs- und Alarmierungssysteme. Hier sind PaaS-Systeme gegenüber SaaS-Systemen klar stärker, wobei es auch bei SaaS-Systemen Automatisierungs- und Integrationsmöglichkeiten gibt.

Ein spezielles Umsystem ist das Identity- und Access-Management-System (IAM). Hier muss klar definiert werden, welchen Anforderungen dieses System genügen muss, etwa Single-Sign-On, Federation und B2B-Integration sowie Multi-Factor-Authentication und Self-Service-Funktionalitäten. Komplexe Mandantenfähigkeit stellt zudem weitere Anforderungen an die Benutzerverwaltung und das IAM.

Folgende Fragen helfen bei der Wahl des richtigen IoT-Cloud-Anbieters in diesem Bereich. Prüfen Sie bei jeder Frage, wie wichtig sie für Ihr Projekt ist (Relevanz) und wie gut der Anbieter diesen Punkt erfüllt (Erfüllungsgrad).

Tabelle 7

	Relevanz	Erfüllungsgrad
Welche Anforderungen an die Mandantenfähigkeit (Multi Tenancy) gibt es und werden diese von der Plattform bereits erfüllt?		
Wie schnell und stark kann die Plattform an zukünftige Anforderungen angepasst werden?		
Können notwendige Anbindungen/Integrationen implementiert werden?		
Sind es proprietäre oder offene Lösungen?		
Probleme entstehen häufig an Schnittstellen: Wie fehlertolerant/resilient sind die Integrationsschnittstellen?		

11 SICHERHEIT (SECURITY)

Sicherheit wurde in der Vergangenheit im IoT-Bereich oft vernachlässigt, insbesondere auf der Device-Seite. Devices wurden einfach ans öffentliche Internet angeschlossen, obschon diese nie entsprechend gehärtet (gesichert) wurden. IoT-Sicherheit ist ein grosses Feld, das hier nicht abschliessend behandelt wird.

Für die Evaluation der Plattform ist in Bezug auf Sicherheit jedoch Folgendes zu beachten:

- Um die Sicherheit von Softwaresystemen zu gewährleisten, gibt es entsprechende Vorgehensmodelle, diese starten typischerweise mit einer Risikoanalyse. Falls Sie diese Modelle nicht kennen, lassen Sie sich von einem Spezialisten beraten.
- Wenn Devices ans Internet angeschlossen werden, muss es zwingend eine Möglichkeit geben, den Kommunikationsstack dieser Devices schnell patchen zu können. Dies für den Fall, dass unbekannte Sicherheitslücken (sogenannte Zero-Days-Vulnerabilities) auftreten. Es gibt beispielsweise noch heute viele verbundene Devices, welche anfällig für die bereits 2014 entdeckte Sicherheitslücke «Heartbeat» in Open SSL sind, aber bis heute nicht gepatched werden konnten (vergleiche auch Kapitel «Konnektivität»).
- Cloud-seitig sollten hohe Standards für die Sicherheit durch die Plattform gewährleistet werden. Achten Sie auf entsprechende Complicance-Zertifizierungen (ISO, SOC, …) sowie auf verschiedene Cloud-Sicherheitsinitiativen (z. B. Cloud Security Alliance).
- Ein besonderes Augenmerk gilt den «public facing interfaces», also den Schnittstellen zu den Devices, zu Umsystemen und zur Benutzerschnittstelle. Für diese Schnittstellen müssen Risikoanalysen gemacht und entsprechende Massnahmen ergriffen werden.

- Weitere kritische Funktionalitäten sind Remote-Update und Remote-Operation. Auch hier benötigt es spezifische Risikoanalysen.
- Wichtig ist zudem das Identity- und Access-Management-System IAM. Dieses sollte modernen, offenen Standards entsprechen (Stichworte sind etwa Claims-basierte Authentifizierung und Multi-Factor-Authentication).

Folgende Fragen helfen bei der Wahl des richtigen IoT-Cloud-Anbieters in diesem Bereich. Prüfen Sie bei jeder Frage, wie wichtig sie für Ihr Projekt ist (Relevanz) und wie gut der Anbieter diesen Punkt erfüllt (Erfüllungsgrad).

Tabelle 8

	Relevanz	Erfüllungsgrad
Werden allgemein anerkannte Best Practices zu Datenschutz und Datensicherheit eingehalten: Verschlüsselung, Zugriffsrechte, Protokolle, Audit?		
Bietet die Plattform bereits benötigte Sicherheitszertifizierungen?		
Wie ausgereift ist der Prozess für das Erkennen und Patchen von Sicherheitslücken?		
Wie schnell kann einem Device der Cloud-Zugriff entzogen werden?		
Welche Anforderungen an das IAM gibt es und erfüllt die Plattform diese Anforderungen?		

12 ABHÄNGIGKEIT VOM ANBIETER (VENDOR-LOCK-IN)

Das Problem des Vendor-Lock-in wurde bereits genannt: Je mehr Funktionalität von einem Cloud-Anbieter genutzt wird, desto schwieriger ist es, zu wechseln. Hier ist aber wichtig abzuklären, ob das Unternehmen nicht bereits eine Abhängigkeit von einem Cloud-Anbieter eingegangen ist: Wenn beispielsweise Office 365 von Microsoft genutzt wird, ist bereits eine Abhängigkeit von Microsoft da. In dem Fall könnte die Strategie darin bestehen, dass auch der IoT-Workload auf der Azure-Cloud umgesetzt und von Rabatten (z. B. Microsoft Enterprise Agreement) und Synergien (z. B. Microsoft Azure Active Directory) profitiert wird. Eine Technologie, die es erlaubt, möglichst viel von der Cloud-Plattform zu nutzen und dennoch unabhängig zu bleiben, sind Containers. Daneben gibt es auch Cloud-Systeme, welche auf Open Source basieren, etwa Openstack oder Cloud Foundry. Die IoT- und Big-Data-spezifischen Dienste auf diesen Plattformen sind jedoch ungenügend.

Folgende Fragen helfen bei der Wahl des richtigen IoT-Cloud-Anbieters in diesem Bereich. Prüfen Sie bei jeder Frage, wie wichtig sie für Ihr Projekt ist (Relevanz) und wie gut der Anbieter diesen Punkt erfüllt (Erfüllungsgrad).

Tabelle 9

	Relevanz	Erfüllungsgrad
Gibt es eine allgemeine Cloud-Strategie im eigenen Unternehmen? Falls ja: Ist die Plattform damit kompatibel?		
Wie hoch ist die technische Abhängigkeit vom Anbieter?		
Wie hoch ist die rechtliche Abhängigkeit vom Anbieter? Wie schnell können Verträge gekündigt werden?		
Besteht bereits eine Abhängigkeit vom Anbieter?		
Gibt es die Möglichkeit, von Rabatten profitieren zu können?		
Werden Container-Technologien unterstützt?		
Werden Open-Source-Technologien unterstützt?		

13 CHINA UND SOVEREIGN CLOUDS

Immer mehr Staaten schränken die Nutzung von ausländischen Cloud-Services ein, beispielsweise China. Dieser Protektionismus ist sowohl technischer als auch rechtlicher Natur. Bei der Auswahl des Cloud-Anbieters muss diese Tatsache berücksichtigt werden, sofern Länder mit entsprechenden Einschränkungen zu den potenziellen Absatzmärkten gehören.

So sind in China sämtliche Cloud-Services von Google nicht erreichbar. Dies betrifft sowohl die Google-Cloud-Plattform als auch beliebte Dienste wie Google Maps, Google Firebase, das für Push-Nachrichten auf Mobile-Apps verwendet wird, und das Google Content Delivery Network, auf welchem beispielsweise Schriftarten hinterlegt sind. Auch können ausländische Unternehmen für ihre Webapplikationen nicht einfach eine Domäne in China beantragen. Dies ist Unternehmen vorenthalten, die mehrheitlich in chinesischem Besitz sind. Weiter gibt es diverse Gesetze zum Umgang mit Daten und deren Verarbeitung. Verstösse werden schnell geahndet und der Zugang zu fehlbaren Webseiten wird blockiert. Der grenzüberschreitende Datenverkehr wird überwacht und VPN-Verbindungen müssen über einen staatlich lizenzierten VPN-Dienstleister bezogen werden.

Es gibt ein Azure China und ein AWS China, die jeweils in mehreren Datencentern in China laufen, aber von chinesischen Anbietern betrieben werden. Diese sogenannten «Sovereign Clouds» sind komplett von Azure und AWS entkoppelt und bieten nur ein Subset der Cloud-Dienste an. Da chinesische Kunden jedoch ein Hosting auf einer rein chinesischen Plattform bevorzugen, ist eine häufige Strategie, das IoT-Backend in China auf einem chinesischen Cloud-Anbieter zu betreiben. Hier haben sich zwei Anbieter etabliert: Alibaba Cloud und Tencent Cloud. Daneben

gäbe es noch HUAWEI und Baidu, diese werden von westlichen Unternehmen aber gemieden, im Fall von HUAWEI wegen Sanktionen der USA. Erfahrungen von europäischen Unternehmen mit den chinesischen Cloud-Anbietern sind durchzogen. Es gibt zwar einen guten Support und die Anbieter versuchen einen einfachen Zugang zu gewährleisten, aber die Dokumentation ist mehrheitlich auf Chinesisch und zum Teil fehlen angepriesene Funktionalitäten.

Bei einer Multi-Cloud-Strategie muss beachtet werden, dass es Teile einer IoT-Architektur gibt, die nicht beliebig auf jeder Cloud laufen. So ist es möglich, die Business-Logik zu containerisieren und auf jede Cloud zu deployen, die beispielsweise Kubernetes unterstützt. Für die Connectivity und das Device-Lifecycle-Management werden häufig proprietäre Cloud-Services verwendet (Azure IoT Hub, AWS IoT Core etc.), welche durch vergleichbare Dienste eines chinesischen Anbieters ersetzt werden müssten, was zu Mehrkosten in der Entwicklung und im Betrieb führt. Hier sind Multi-Cloud-fähige SaaS-IoT-Plattformen wie Cumulocity IoT im Vorteil, da sie auf jeder Public-Cloud betrieben werden können.

Auch für die Speicherung und Verarbeitung von Big Data werden häufig proprietäre Services einer bestimmten Cloud genutzt, da diese kosteneffizient sind. Die einfachste Strategie ist, die Daten aus allen Ländern zentral zu speichern und zu verarbeiten, etwa indem (anonymisierte) Daten aus China nach Europa gesendet werden. Falls dies nicht möglich ist, muss hier mit erheblichen Mehrkosten gerechnet werden.

Letztlich ist in Multi-Cloud-Szenarien auch die Integration komplex, etwa mit dem eigenen ERP-System. Dabei muss darauf ge-

achtet werden, welche Meta- oder Kundendaten in das chinesische System exportiert werden, und sichergestellt werden, dass das eigene geistige Eigentum (und das der Kunden) geschützt bleibt.

Neben China gibt es ähnliche Einschränkungen in Russland, Brasilien und Indien.

Folgende Fragen helfen bei der Wahl des richtigen IoT-Cloud-Anbieters in diesem Bereich. Prüfen Sie bei jeder Frage, wie wichtig sie für Ihr Projekt ist (Relevanz) und wie gut der Anbieter diesen Punkt erfüllt (Erfüllungsgrad).

Tabelle 10

	Relevanz	Erfüllungsgrad
Ist das Angebot / die Cloud-Plattform in sämtlichen geografischen Absatzmärkten verfügbar?		
Sind alle voraussichtlich genutzten Cloud-Dienste in allen Absatzländern verfügbar?		
Wie gut ist die Unterstützung durch den Cloud-Anbieter beim Deployment und dem Betrieb der Lösung in nationalen Clouds?		
Vervielfachen sich die Kosten beim Deployment und Betrieb der Lösung in nationalen Clouds?		
Unterstützt die Cloud-Plattform meine Strategie für China und andere Länder mit Einschränkungen?		

14 STRATEGIE DES IOT-PLATTFORM-BETREIBERS

Achten Sie bei der Wahl der IoT-Plattform auf die Strategie des Anbieters und dessen Kunden-Portfolio. Ganz unglücklich wäre etwa, wenn der Cloud-Anbieter später von Ihrer Konkurrenz aufgekauft wird. Solche Dinge lassen sich natürlich nur beschränkt voraussagen.

Auch bei den grossen Anbietern lohnt es sich, das Marktverhalten zu beobachten: Im Moment versuchen alle Marktteilnehmer mittels Innovationen, sich gegenseitig Marktanteile abzugewinnen, da bleibt die Qualität zum Teil auf der Strecke. Zudem kann es sein, dass ein Cloud-Betreiber heute nicht kostendeckend anbietet, um Kunden zu gewinnen, aber dass dann die Preise mittel- oder langfristig steigen.

Die grossen Anbieter haben zudem Zukäufe getätigt, um ihren Cloud-Bereich zu schützen bzw. auszubauen, etwa Microsoft mit GitHub oder IBM mit Red Hat. Solche Zukäufe wälzen die ganze Branche von einem Tag auf den anderen um und ermöglichen bei den einen Chancen, bei anderen wachsen dagegen die Risiken.

Folgende Fragen helfen bei der Wahl des richtigen IoT-Cloud-Anbieters in diesem Bereich. Prüfen Sie bei jeder Frage, wie wichtig sie für Ihr Projekt ist (Relevanz) und wie gut der Anbieter diesen Punkt erfüllt (Erfüllungsgrad).

Tabelle 11

	Relevanz	Erfüllungs-grad
Ist die Strategie des Anbieters bekannt?		
Passt die Strategie des Anbieters zur eigenen Strategie?		

15 MATURITÄT / ENTERPRISE READINESS

Wer mittel- und langfristig denkt, für den ist klar, dass die gewählte IoT-Plattform eine gewisse Maturität besitzen muss, man spricht dabei auch von «Enterprise Readiness». Dazu gehören verschiedene Punkte: das Ökosystem, die Community, Prozesse des Plattform-Betreibers und die User Experience und Compliance.

Bei der Maturität spielt das Ökosystem für die Softwareentwickler eine wichtige Rolle. Damit ist zum Beispiel gemeint, dass Entwickler nicht direkt auf einer produktiven Umgebung entwickeln müssen, sondern eine Entwicklungs-, Test- und Integrationsumgebung zur Verfügung haben, inklusive Werkzeuge für Continuous Integration, Continuous Deployment, Sicherheit und DevOps.

Es gehört auch eine Community dazu: Wie einfach können auf dem Markt Softwareentwickler gefunden werden, die die Lösung weiterentwickeln können? Wie schnell erhält man Hilfe bei einem Problem – durch den Anbieter oder die Community?

Zur Enterprise Readiness gehören aber auch die Prozesse des Plattform-Betreibers: Wie kompliziert ist das Onboarding? Wie schnell können neue Ressourcen provisioniert werden? Können Sie per Rechnung bezahlen statt per Kreditkarte? Welches SLA erhalten Sie?

Bei SaaS-Plattformen gehört zur Enterprise Readiness auch die User Experience: Dabei geht es darum, wie intuitiv und schnell eine Benutzeroberfläche erlernbar ist und ob der Benutzer alle Funktionalitäten, die er braucht, schnell auffindet. Solche Dinge werden immer häufiger zum entscheidenden Wettbewerbsvorteil von Softwarelösungen. Und letztlich sollte es rund um die Plattform ein Ökosystem an Integrationslösungen geben.

Folgende Fragen helfen bei der Wahl des richtigen IoT-Cloud-Anbieters in diesem Bereich. Prüfen Sie bei jeder Frage, wie wichtig sie für Ihr Projekt ist (Relevanz) und wie gut der Anbieter diesen Punkt erfüllt (Erfüllungsgrad).

Tabelle 12

	Relevanz	Erfüllungsgrad
Unterstützt die Plattform einen modernen Entwicklungsprozess?		
Unterstützt die Plattform einen modernen Testing-/Qualitätssicherungsprozess?		
Unterstützt die Plattform einen modernen Release-Prozess/Continuous Deployment/DevOps?		
Wie gross ist die Entwickler-Community?		
Wie gut ist der Support (Reaktionszeiten/Qualität der Antworten)?		
SaaS: Bietet die Plattform ein modernes User-Interface (z. B. Mobile-fähig)?		
Erfüllt die Plattform die essenziellen Charakteristiken für Cloud-Computing gemäss NIST?		

16 COMPLIANCE

Das Thema Compliance betrifft die verschiedenen Security-, Datenschutz- und Branchen-Standards. Hierbei muss ein besonderes Augenmerk auf Abhängigkeiten gerichtet werden: Wenn beispielsweise die IoT-Plattform keine ISO/IEC-27001-Zertifizierung aufweist, werden Sie es schwer haben, Ihre darauf basierende Lösung diesbezüglich zu zertifizieren. Dasselbe gilt beispielsweise für den Datenschutz (etwa GDPR-Compliance) oder andere branchenspezifische Standards. Überlegen Sie sich bei der Wahl der Plattform, welche Compliance-Zertifizierungen Sie Ihren Kunden in Zukunft anbieten wollen bzw. müssen. Es ist zudem ein Markenzeichen von guten Cloud-Plattformen, wenn die Compliance-Zertifizierungen und -Audits mit einer einfachen Web-Suche sofort auffindbar sind, was selbst bei grossen Anbietern nicht immer der Fall ist.

Folgende Fragen helfen bei der Wahl des richtigen IoT-Cloud-Anbieters in diesem Bereich. Prüfen Sie bei jeder Frage, wie wichtig sie für Ihr Projekt ist (Relevanz) und wie gut der Anbieter diesen Punkt erfüllt (Erfüllungsgrad).

Tabelle 13

	Relevanz	Erfüllungsgrad
Erfüllt der Anbieter branchenspezifische Regularien?		
Welche allgemeinen Compliance-Standards müssen eingehalten werden und erfüllt die Plattform diese Standards bereits?		
Wie stark unterstützt mich die Plattform bei eigenen Zertifizierungen/Audits, zum Beispiel in Form von Checklisten und Gap-Analysen?		
Müssen meine Daten an einem bestimmten Ort/in einem bestimmten Land gespeichert sein? Erfüllt der Cloud-Anbieter diese Anforderung?		

17 VERTRAG UND SLA

Wie bei der Compliance ist auch beim SLA die Abhängigkeit zu beachten: Sie können im SLA, das sie Ihren Kunden ausstellen, keine höhere Verfügbarkeit (Uptime & Mean time to Recovery) gewährleisten, als Sie im SLA von Ihrem Provider garantiert bekommen. Das Provider-SLA hat somit direkte Auswirkungen auf das SLA, das Sie anbieten können. Zudem ist es wichtig zu verstehen, dass Cloud-Anbieter bei Verletzung des SLAs in der Regel keinen Schadensersatz bezahlen.

Neben dem SLA des Cloud-Anbieters sind aber auch dessen Vertrag und die Geschäftsbedingungen wichtig. In diesem Vertrag muss unter anderem geregelt sein, dass die Daten nicht dem Cloud-Anbieter gehören und dieser keine Rechte an den Daten hat. Spezialisierte Juristen können hier unterstützen.

Folgende Fragen helfen bei der Wahl des richtigen IoT-Cloud-Anbieters in diesem Bereich. Prüfen Sie bei jeder Frage, wie wichtig sie für Ihr Projekt ist (Relevanz) und wie gut der Anbieter diesen Punkt erfüllt (Erfüllungsgrad).

Tabelle 14

	Relevanz	Erfüllungsgrad
Sind die Bedingungen des SLA akzeptabel?		
Sind die spezifischen und allgemeinen Vertragsbedingungen akzeptabel?		
Welche Entschädigung leistet der Anbieter im Fall des Nicht-Einhaltens des SLA?		

18 KOSTEN

Die Kosten sind bei SaaS-Plattformen in der Regel einfach zu berechnen. Diese Plattformen rechnen pro Device und/oder pro Benutzer ab. Sind die Pricing-Informationen bei einer SaaS-Lösung nicht transparent, könnte das darauf hinweisen, dass es sich eigentlich um eine IoT-Dienstleistung handelt oder dass die Cloud-Plattform eine ungenügende Maturität/Automatisierung aufweist.

Bei den PaaS-Lösungen werden die Preise pro Cloud-Dienst abgerechnet, der benutzt wird. Dies ist zwar auch transparent, aber sehr komplex, da eine fertige Architektur aus vielen verschiedenen Services besteht und ein detailliertes Mengengerüst nötig ist, um die Kosten berechnen zu können. Bei PaaS kommen zudem noch Aufwendungen für den Betrieb hinzu.

Bei allen Cloud-Lösungen gilt: Preise können relativ kurzfristig vom Anbieter geändert werden. Uns ist kein Cloud-Anbieter bekannt, der die Preise über mehr als drei Jahre vertraglich zusichert.

Folgende Fragen helfen bei der Wahl des richtigen IoT-Cloud-Anbieters in dieser Phase. Prüfen Sie bei jeder Frage, wie wichtig sie für Ihr Projekt ist (Relevanz) und wie gut der Anbieter diesen Punkt erfüllt (Erfüllungsgrad).

Tabelle 15

	Relevanz	Erfüllungsgrad
Müssen Preise verhandelt werden oder sind sie transparent?		
Wie stabil sind die Preise über die Zeit?		
Wie skalieren die Preise?		
Wie schnell reagiert der Cloud-Anbieter bei Verringerung des Mengengerüsts? Werden Kosten live abgerechnet oder muss man jedes Mal bis Ende Monat/Quartal/Jahr warten?		
In welcher Währung erfolgt die Abrechnung (Abgleich mit Buchhaltung)?		
Gibt es Hilfsmittel zur Berechnung der Kosten?		
Gibt es weitere Kosten wie z. B. Lizenzen für SDK oder Ähnliches?		

19 CHECKLISTE FÜR DEN BETRIEB VON IOT-CLOUD-LÖSUNGEN

Um eine Plattform zu evaluieren, ist es wichtig, eine Gesamtkostenrechnung aufzustellen. Dabei gibt es neben dem Entwicklungsaufwand und den Preisen des Cloud-Anbieters einige versteckte Aufgaben, die zu Beginn eines Projekts oft vergessen gehen oder unterschätzt werden.

Folgende Checkliste dient dazu, die zusätzlichen Aufwendungen sichtbar zu machen, die es für den Betrieb einer IoT-Lösung braucht. Diese Liste ist nur Cloud-seitig anwendbar und grob an ITIL/ISO 20000 angelehnt. Die Checkliste basiert auf Erfahrungen aus verschiedenen Projekten, hat aber keinen Anspruch auf Vollständigkeit.

Bei SaaS-Plattformen wird ein Grossteil dieser Aufgaben durch den Betreiber übernommen. Es lohnt sich jedoch, sowohl bei PaaS als auch bei SaaS mit dem Betreiber zu klären, wer verantwortlich für welche dieser Aufgaben ist.

19.1 APPLICATION LIFECYCLE MANAGEMENT

- Einrichten und Betrieb von Development/Test/Integrations-Umgebungen
- Lizenzkosten für Development Tools (IDE, Build-Server usw.)
- Einrichten und Betrieb von CI/CD-Pipelines
- Einrichten und Betrieb von Infrastructure-as-Code/Automation
- Projekt- und Release-Planning

19.2 SUPPORT AN DEN ENDKUNDEN

- Support-Organisation
  - First Level, Second Level, Third Level
  - Antwortzeiten (7/24, Business-Hours)
  - «Best-Effort»

- SLA
  - Verfügbarkeit («Up-Time»)
  - Recoverability (MTTR): Daten, Identitäten, Infrastruktur

19.3 APPLICATION MANAGEMENT

- Ausführung von regelmässigen Wartungs- und Administrationsarbeiten (sofern nicht automatisiert), zum Beispiel:
  - SSL-Zertifikate erneuern, DNS-Hosting-Administration
  - Verwaltung und Austausch von kryptografischem Material
  - Regelmässige Schlüsselerneuerung (Key Rollover)
  - Prüfen von Backup- und Restore-Szenarien
  - Datenbereinigung, Datenarchivierung, Retention
  - DBA-Tasks: Datenbank-Indices und Statistics optimieren
  - Housekeeping, ausführen von manuellen Jobs
- Multi Tenancy/Mandantenfähigkeit
  - Onboarding von neuen Mandanten
  - Prüfen von gelöschten Mandanten gemäss Compliance-Vorgaben (auch im Backup gelöscht)
  - Verwaltung von Benutzern, Rollen und Rechten, soweit nicht über Self-Service abgedeckt
- Wartungsfenster
  - Wartungsfenster planen, kommunizieren und durchführen
  - Management von angekündigten Wartungsfenstern des Cloud-Providers
- Globale Verteilung (sofern nötig)
  - Steuerung der geografischen Verteilung des Systems
  - Geo-Load-Balancer, Content Delivery Network
  - Management von Geo-Replikation der Applikation und der Daten
  - Etablierung von Desaster-Recovery-/Business-Continuity-Plänen

- Security
  - Prozess für das Sperren oder Löschen eines Device, wenn ein Device oder Device-Zugangsdaten kompromittiert wurden
  - Auswertung von Empfehlungen von Cloud-Advisory Tools (Performance, Security usw.)
- Betrieb von IaaS-Komponenten sofern vorhanden
  - Einspielen von Updates für Betriebssystem und Applikationen

19.4 COMPLICANCE & AUDIT

Je nach angestrebter Auditierung/Compliance-Standard:

- Know-how-Aufbau zu den Anforderungen des Audits
- Vorbereiten des Audits (regelmässig)
- Unterstützung des Auditors bei der Durchführung
- Implementation der Compliance-Vorgaben/-Policies in den Prozessen und Dokumentationen
- Zusammenarbeit bei der Vertragsgestaltung/Ausarbeitung SLA mit entsprechenden Abteilungen
- Export von Kundendaten auf Wunsch
- Technische Behandlung von regulatorischen Anforderungen
- Technische Behandlung von Behördenanfragen (namentlich Regulierungs- und Justizbehörden)
- Beobachtung, Planung und Umsetzung von neuen oder geänderten regulatorischen Anforderungen
- Penetrationstests organisieren

19.5 MONITORING

- Überwachung der Log-Dateien
- Alerts einrichten und verwalten
- Überwachen von Quotas/Throttling-Grenzen, manuelles/automatisiertes Scaling einrichten

- Frühzeitiges Erkennen und Beantragen von benötigten Subscription-Quota-Erhöhungen
- Monitoring und Dokumentation von Metrics/KPIs (Uptime, Responsetime, Usage)
  – Relevant für SLA
  – Relevant für Rechnungsstellung
- Job Monitoring und Überwachung von Dead-Letter-Queues
- Überwachung der angebundenen Nicht-Cloud-Systeme (z. B. ERP)

19.6 PROBLEM-/INCIDENT MANAGEMENT:

- Kommunikation von Ausfällen/Incidents/Störungen/Problemen und Absprache mit dem 3. Level Support/Entwicklungsteam
- Unterstützung in der Diagnose und im Problemlösungsprozess
- Rasche Kommunikation von (Teil-)Ausfällen oder Störungen der Cloud-Plattform

19.7 RELEASE MANAGEMENT

- Release-Planung
- Deployments vorbereiten, durchführen
- Ggf. Aufbau eines DevOps-Teams

19.8 CHANGE MANAGEMENT

Upgrade-Administration bei Anpassungen/Neuerungen der Cloud-Plattform

19.9 BILLING & SUBSCRIPTION MANAGEMENT

- Verantwortung für das Subscription Management
  – Steuerung der Zugriffsrechte für Entwickler, Data Scientists, Drittsysteme etc.
  – Verwaltung des Enterprise-Agreements

- Kostenüberwachung und Kontrolle der Rechnungen seitens Cloud-Provider
- Aufbereitung der Grundlagen für die Rechnungstellung an die Mandanten (sofern nicht automatisiert)
- Re-Evaluation der Gesamtarchitektur bei Kostenänderungen an einzelnen Cloud-Services

19.10 WEITERE AUFGABEN

- Dokumentation, Schulung von neuen Mitarbeitern, Know-how-Management
- Im Falle von speziellen, einmaligen Auswertungen (z. B. durch Data Scientists): Unterstützung beim Datenzugriff

bbv
MAKING VISIONS WORK.

bbv Software Services AG ist ein Schweizer Software- und Beratungsunternehmen, das Kunden bei der Realisierung ihrer Visionen und Projekte unterstützt. Wir entwickeln individuelle Softwarelösungen und begleiten Kunden mit fundierter Beratung, erstklassigem Software Engineering und langjähriger Branchenerfahrung auf dem Weg zur erfolgreichen Lösung.

Unsere Booklets und vieles mehr finden Sie unter
www.bbv.ch/publikationen

MAKING VISIONS WORK.

www.bbv.ch · info@bbv.ch