Ausgabe **03/2021**

Industrial-IoT-Cloud-Lösung

Worauf Sie bei der Auswahl achten sollten:

Whitepaper inkl. Checkliste

adstec
Industrial IT

Marc Schmierer, seit 2017 bei der ads-tec Industrial IT GmbH als Produktmanager und Spezialist für IIoT-Cloud-Lösungen

Vorwort

Trotz des großen Wachstumspotenzials liegt die Digitalisierungsrate in der Produktion deutscher Großunternehmen erst bei knapp 30 Prozent – bei kleinen und mittleren Unternehmen sogar nur bei 20 Prozent[1]. Ein Grund dafür könnte die große Anzahl an Anbietern von Industrial IoT-Cloud-Lösungen sein. Gut, wenn man weiß, worauf man bei der Auswahl achten muss.

In Zeiten von Industrie 4.0 und der stetigen Vernetzung von Personen und Geräten wundert es wenig, dass sich immer mehr Unternehmen mit dem Thema Industrial-IoT auseinandersetzen und nach passenden Lösungen suchen. Gleichzeitig wirft das Thema bei vielen Unternehmen auch eine Menge Fragen auf: Nehme ich eine reine Fernwartungslösung? Oder doch besser eine komplette Industrial IoT-Cloud-Lösung? Und überhaupt: Was ist die richtige Lösung für mich?

Dieses Whitepaper beleuchtet die unserer Erfahrung nach geläufigsten Gesichtspunkte, die bei der Auswahl beachtet werden sollten. Am Ende des Whitepapers finden Sie zusätzlich eine Checkliste, die Ihnen bei der Bewertung und Entscheidung sowie der letztendlichen Auswahl Ihrer zukünftigen Industrial-IoT-Lösung sicherlich helfen wird.

Marc Schmierer
ads-tec Industrial IT GmbH

Inhalt

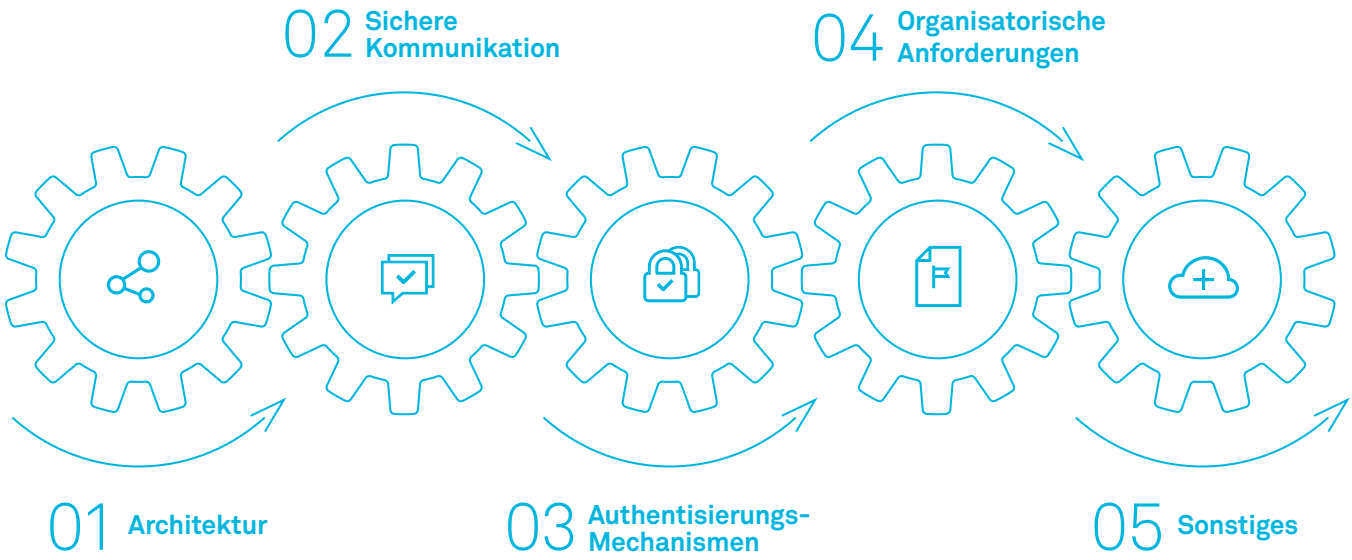
Security-Standard

Bietet die Lösung optimalen Schutz für Ihre Maschinen- & Unternehmensdaten?

Achten Sie darauf, dass Ihre IIoT-Lösung die empfohlenen Richtlinien des BSI beachtet.

Einer der wichtigsten Faktoren und für viele Unternehmen sogar der wichtigste Faktor bei der Suche nach einer IIoT-Lösung ist die Sicherheitsfrage. Niemand möchte das Risiko eingehen, dass sein Unternehmen und seine Maschinen gehackt und sensible Daten gestohlen oder Prozesse gestört werden.
Die zentrale Frage, mit der Sie sich bei der Suche nach einem IIoT-Anbieter beschäftigen sollten, lautet also: Wie hoch wird die Security der Lösung beim jeweiligen Anbieter angesetzt? Zum Schutz der Maschinen- und Anlagendaten hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) Richtlinien bestimmt, an welche sich IIoT-Anbieter orientieren können.

BSI-Richtlinien zum Schutz der Maschinen- und Anlagendaten



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI), Stand September 2020

01 Architektur

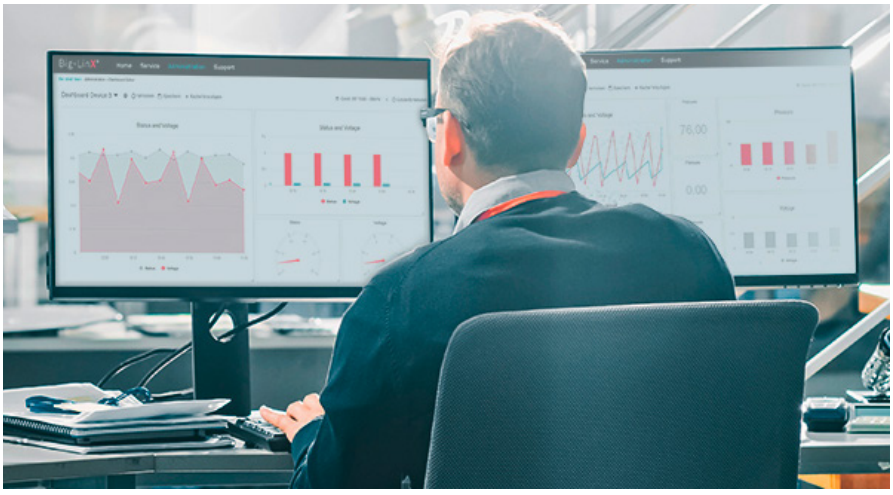
Wie sicher eine industrielle Fernwartungslösung letztendlich ist, hängt maßgeblich von ihrer Architektur ab. Aus diesem Grund sollten bereits bei der Planung und Integration einer Fernwartungslösung einige Anforderungen beachtet werden.

Einheitliche Lösung
Um die Gefahr eines Hackerangriffs zu reduzieren, sollten Sie „Wildwuchs“ vermeiden.

Fernwartungskomponenten im DMZ
Die Fernwartungskomponenten sollten sich in einer vorgelagerten Demilitarisierten Zone (DMZ) befinden und nicht im Produktionsnetz. Mit Hilfe von Firewalls kann exakt definiert werden, auf welche Geräte zugegriffen werden darf.

Granularität der Kommunikationsverbindungen
Der Fernzugriff sollte auf ein Minimum beschränkt werden, sprich ein Zugriff pro IP und Port, da hierdurch die Reichweite eines möglichen Angriffs reduziert werden kann.

Verbindungsaufbau
Die Verbindung sollte ausschließlich von intern (z. B. Unternehmensnetzwerk) zu extern (z. B. Fernwartungsserver) aufgebaut werden.



75%

der IT- & Security-Experten sehen in der Zunahme von Cyber-Angriffen ihre größte Sorge während der Pandemie [2]

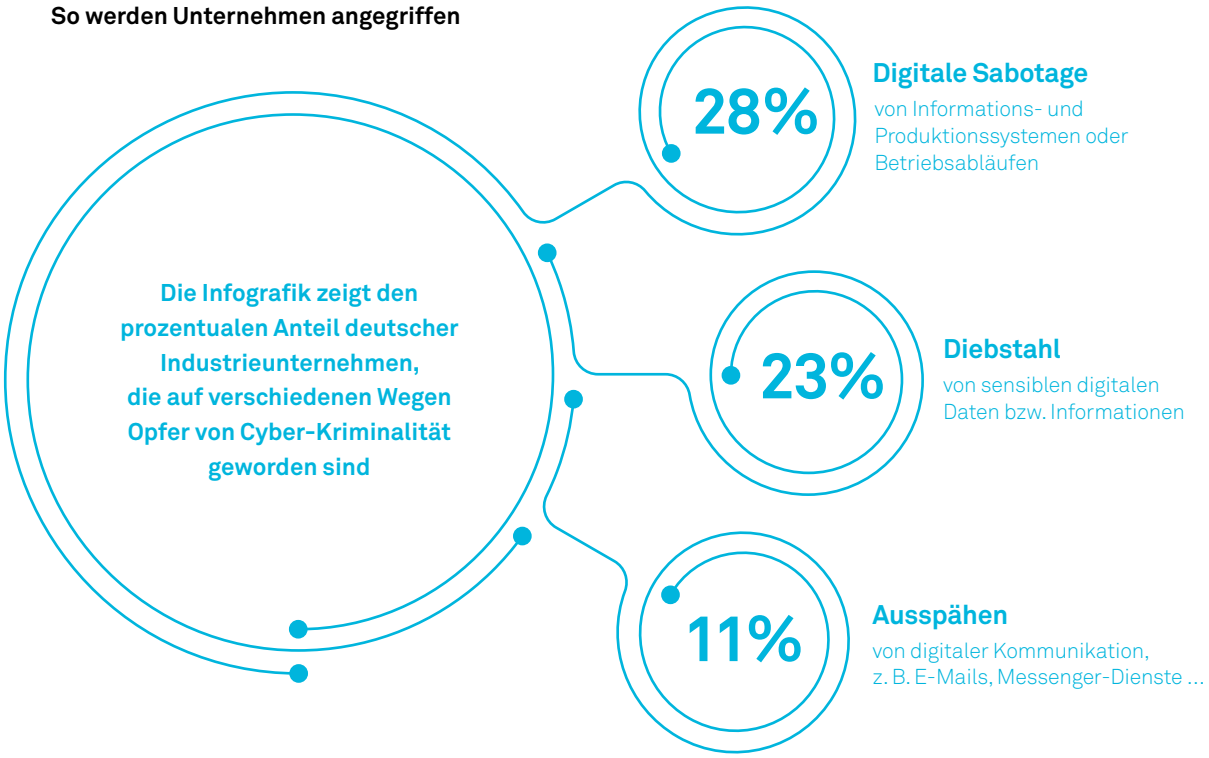
02 Sichere Kommunikation

Ein weiterer relevanter Punkt zum Schutz von Maschinen- und Anlagendaten stellt die Kommunikation bzw. die Kommunikationswege dar. Die Sicherheit dieser wird durch etablierte Standardlösungen gewährleistet.

Sichere Protokolle
Wählen Sie einen Anbieter mit etablierten Protokollen. Zu empfehlen sind: TLS (OpenVPN), IPsec oder SSH in der jeweils aktuellsten Version.

Sichere Verfahren
Eine Verbindung zur Maschine oder Anlage sollte mit einem starken kryptographischen Verfahren verschlüsselt sein. Zu den starken Verbindungen zählen Schlüssellängen von AES mit mindestens 192 Bit.

So werden Unternehmen angegriffen



Quelle: Bitcom Research, Studie zum Thema „Cyber-Kriminalität in deutschen Unternehmen“ , Stand 2019

03 Authentisierungs-Mechanismen

Die sichere und zuverlässige Authentisierung der Nutzer ist ein wichtiger Punkt beim Schutz von Maschinen- und Anlagendaten. Nur wenn diese gewährleistet ist, kann ein ausreichendes Sicherheitsniveau für industrielle Fernwartung geschaffen werden.

Granularität der Accounts
Sie sollten unbedingt auf Gruppen-Accounts verzichten und nur einen Anbieter auswählen, bei dem jeder Benutzer einen Account hat.

Starke Authentisierungsmechanismen
Für ein maximales Sicherheitsniveau sollte die Authentisierung nicht via Passwort, sondern via einer Zwei-Faktor-Authentifizierung ablaufen. Bei Hardware-basierten Lösungen ist zu empfehlen Anbieter mit Smartcards, USB-Token oder Einmal-passwörtern zu verwenden, da hier das Kopieren von Hardwarekomponenten nicht möglich ist.

04 Organisatorische Anforderungen

Architektur und Technik sind zwar tragende Säulen beim Schutz von Maschinen- und Anlagendaten, aber um maximale Sicherheit zu gewährleisten, sind auch Maßnahmen zu ergreifen, die eine sichere Integration und einen sicheren Betrieb garantieren.

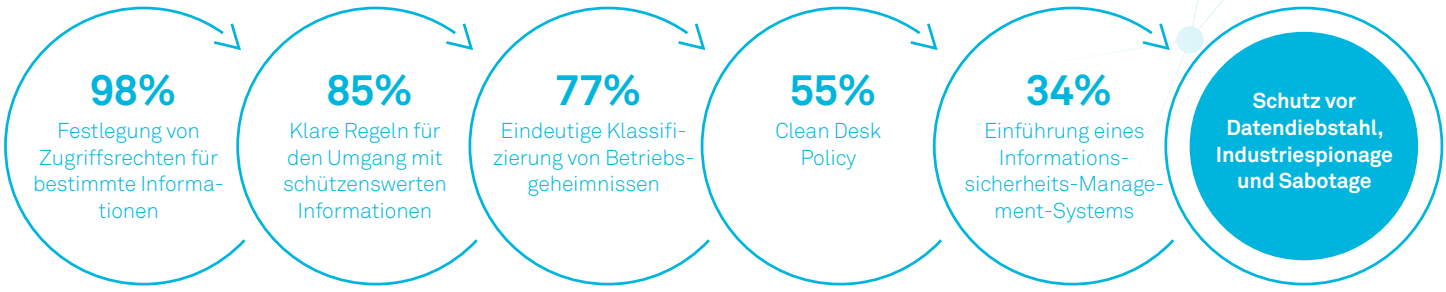
Inventarisierung
Die Zugriffe auf die Geräte sollten erfasst werden, sprich es muss lückenlos nachvollziehbar sein, wer, wann und wie lange mit einem Gerät verbunden war.

Zeitfenster
Der Zugang zur Maschine oder Anlage erfolgt entweder bei einer Störung oder durch die Festlegung eines Zeitfensters (z. B. Schlüsselschalter). In beiden Fällen ist die Aktivierung bzw. Deaktivierung zu dokumentieren.

Patchprozess
Die Komponenten sollten patchfähig sein, damit eine wichtige eventuelle Schwachstelle schnell behoben werden kann.

Logging & Alerting
Der Anbieter der Lösung sollte Anmeldungen protokollieren und ggf. Alarme generieren.

Organisatorische Maßnahmen im Einsatz
Neben technischen Voraussetzungen sind es insbesondere organisatorische Maßnahmen, die sich auf den Sicherheitsstandard einer IIoT-Lösung auswirkt. Die Ergebnisse dieser Studie, bei der über 1.000 Unternehmen befragt wurden, zeigen deutlich, welche organisatorischen Sicherheitsvorkehrungen in Unternehmen zum Einsatz kommen, um sich gegen Datendiebstahl, Industriespionage und Sabotage zu schützen.



Quelle: Bitcom Research, Studienbericht 2020 „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt“

05 Sonstiges

Je nach Anwendungsfall können auch weitere individuelle Maßnahmen getroffen werden, um die Sicherheit der Fernwartungslösung zu gewährleisten.

Skalierbarkeit
Die Lösung sollte sich auf verändernde Verhältnisse, wie die Anzahl der Maschinen und Anlagen, aber auch auf bereits bestehende Maschinen und Brownfield-Maschinen anpassen können.

Investitionsschutz
Ein weiteres Kriterium für die Auswahl der IIoT-Service-Plattform ist, ob zukünftige Anforderungen berücksichtigt werden.

IT Security made in Germany

Bei Erfüllung bestimmter Kriterien haben IIoT-Anbieter die Möglichkeit, sich vom Bundesverband IT-Sicherheit e. V. (TeleTrust) mit dem Vertrauenszeichens „IT Security made in Germany“ auszeichnen zu lassen. Die TeleTrust mit Sitz in Berlin ist für ihre Mitglieder in Deutschland und Europa eine der ersten Anlaufstellen, wenn es um den kompetenten Informationsaustausch zu Themen aus dem Umfeld der IT-Sicherheit geht. In verschiedenen Foren und Veranstaltungen haben die Mitglieder die Möglichkeit, sich zu ändernden Sicherheitsmaßnahmen auszutauschen.
Das Vertrauenszertifikat „IT Security made in Germany“ ist ein Garant für uneingeschränkte, maximale Transparenz und höchste Datensicherheit – alles Made in Germany. Auf diese Art profitieren Sie nicht nur von der Qualität der Lösung, sondern sind auch in puncto Service und Wartung auf der sicheren Seite.

Tipp: Fragen Sie den Anbieter nach seinen Security Guidelines. Hier finden Sie Informationen darüber, welche technischen Konzepte eingesetzt werden, mit welchen Herstellern der Anbieter zusammenarbeitet oder wie Probleme gehandhabt werden.

Anforderungskriterien für Anbieter

1. Der Unternehmenshauptsitz muss in Deutschland sein.
2. Das Unternehmen muss vertrauenswürdige IT-Sicherheitslösungen anbieten.
3. Die angebotenen Produkte dürfen keine versteckten Zugänge ("Backdoors") enthalten.
4. Die IT-Sicherheitsforschung und -entwicklung des Unternehmens muss in Deutschland stattfinden.
5. Das Unternehmen muss sich verpflichten, den Anforderungen des deutschen Datenschutzrechtes zu genügen.

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig

Quelle: Bundesverband IT-Sicherheit e. V.

„Netzwerke sollten mit einer ganzheitlichen, durchgehenden Sicherheitsarchitektur ausgestattet werden.“[2]

Dietmar Schnabel
Regional Director Central Europe bei Check Point Software Technologies GmbH

Funkionalität

Enthält die Lösung alle Funktionalitäten, die Sie für Ihre Arbeit benötigen?

Achten Sie darauf, dass die Lösung sowohl Ihre aktuellen als auch zukünftigen Anforderungen abdeckt

Stellen Sie sich folgendes Szenario vor: Einige Zeit nach der Inbetriebnahme Ihrer Plattform stellen Sie fest, dass Sie weitere Funktionen im IIoT-Bereich benötigen. Diese sind aber in Ihrer Plattform nicht enthalten. Da Sie die Funktionalität aber zwingend benötigen, bleibt Ihnen nichts anderes übrig, als einen weiteren Dienstleister an Ihr Unternehmensnetz anzubinden.
Daher ist es ratsam, bereits im Vorfeld genau zu definieren, welche Funktionalitäten Sie sich von der Lösung wünschen, um späteren „Wildwuchs“ zu vermeiden und das Sicherheitsrisiko nicht unnötig zu erhöhen.

Vorsehen statt Nachsehen
Auf der Suche nach einer IIoT-Lösung werden Sie auf unzählige Anbieter mit verschiedenen Ansätzen stoßen. Die Angebote reichen von VPN-Lösungen über Cloud-basierte Ansätze bis hin zu Provider-Lösungen im Bereich Machine-to-Machine (M2M), wobei sich die Produkteigenschaften einzelner Lösungen dabei teilweise signifikant unterscheiden[3]. Damit Sie den richtigen Anbieter für sich finden, sollten Sie bereits im Vorfeld definieren, welche Funktionalitäten sie aktuell benötigen und welche in der Zukunft eventuell benötigt werden. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät in diesem Zusammenhang zu vorausschauendem Handeln, um späteren „Wildwuchs“ zu vermeiden. Daher sollten Sie bereits bei der Suche genau definieren, ob Sie zu einem späteren Zeitpunkt weitere Funktionalitäten benötigen werden, wie z. B. die nachträgliche Visualisierung und Darstellung von Maschinen- und/oder Anlagendaten in Dashboards.

In diesem Zusammenhang ist es ratsam einen Anbieter zu wählen, dessen Lösung neben dem reinen Fernwartungsaspekt auch zusätzliche IIoT-Funktionalitäten enthält, die Sie flexibel buchen und bei Nichtverwendung wieder stornieren können. So können Sie auf wechselnde Anforderungen schnell reagieren und bezahlen für die zusätzlich gebuchten Funktionalitäten nur so lange, wie Sie diese auch in Anspruch nehmen. In diesem Zusammenhang sind besonders Plattformen mit offenen Schnittstellen wie bspw. REST zu empfehlen. Diese bieten Ihnen bei kunden- und branchenspezifischen Themen, wie z. B. dem Machine Learning, zusätzlichen Investitionsschutz, da zukünftige Dienste direkt an das bestehende System angebunden werden können.

Tipp: Einige Unternehmen bieten in der Konfigurations-Phase Workshops an, um sowohl aktuelle als auch zukünftige Anforderungen zu erfassen und die IIoT-Lösung darauf auszurichten.

Kosten

Welches Preismodell ist das Richtige für Sie und Ihre Anforderungen?

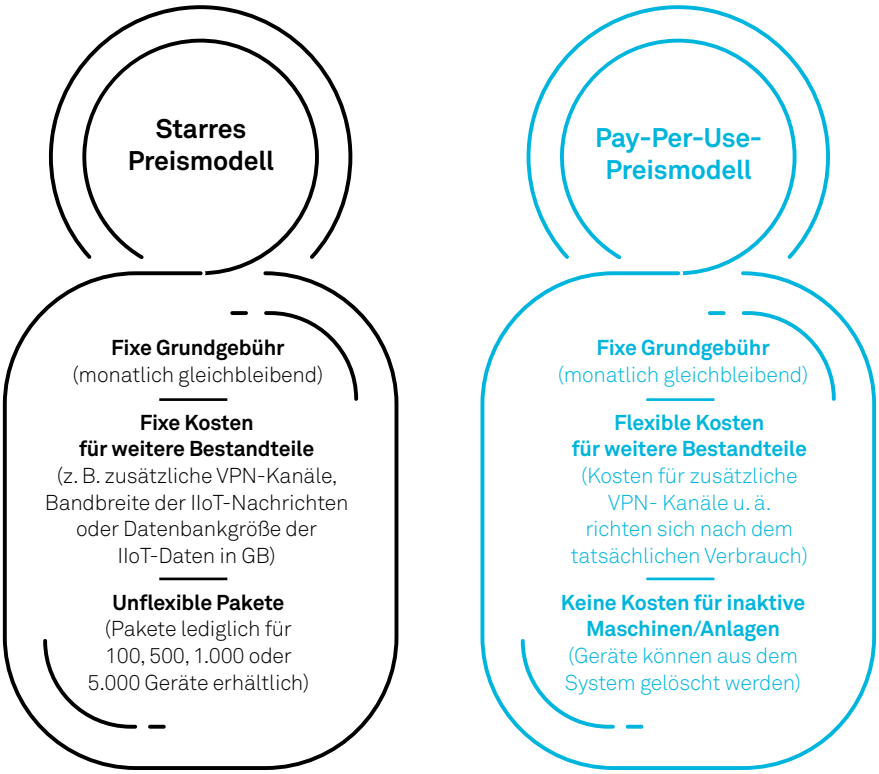
Führen Sie zur besseren Bewertung eine Break-Even-Analyse durch.

Die meisten Anbieter von IIoT-Service-Plattformen bieten zwei Arten von Abrechnungsmodellen an: das starre Preismodell und das flexible Pay-Per-Use-Modell. Doch welches der beiden passt besser zu Ihnen und Ihren Anforderungen?

Bei der finalen Entscheidung, welches dieser beiden Modelle für Sie das Richtige ist, empfiehlt es sich, eine Break-Even-Rechnung durchzuführen. So können sie leicht herausfinden, ab wie vielen Maschinen sich das eine oder das andere Modell für Sie rechnet.

Starres Preismodell vs. Pay-Per-Use-Modell

Nimmt man die beiden gängigen Preismodelle unter die Lupe, lassen sich sowohl Gemeinsamkeiten als auch Unterschiede feststellen. Worin sich die Modelle jedoch unterscheiden, sind die Kosten für weitere Bestandteile wie Instandhaltung, Wartung, Service, Updates sowie die Wahrung der Funktionsfähigkeit der Plattform.



Ein wichtiges Thema bei der Bestimmung des passenden Preismodells sind die Abrechnungsintervalle. Geläufig sind Jahresabrechnungen sowie Monatsabrechnungen, die je nach Benutzerverhalten mal Vorteile und mal Nachteile mit sich bringen. Sollten Sie bspw. den Funktionsumfang Ihrer Lösung häufiger anpassen müssen oder ist davon auszugehen, dass die zu überwachende Maschinenanzahl variieren wird, ist eine monatliche Abrechnung im Rahmen eines Pay-Per-Use-Modells empfehlenswert. So behalten Sie nicht nur Ihre Kosten besser im Blick: Mit diesem Modell gewinnen Sie auch an Planungssicherheit im Vergleich zu einer Jahresabrechnung.

Bei der finalen Entscheidung, welches Preismodell für Sie und Ihre Anforderungen das attraktivere ist, empfehlen wir Ihnen eine Break-Even-Analyse durchzuführen. So können sie individuell ermitteln, ab welcher Anzahl von Maschinen Sie das eine Modell dem anderen bevorzugen sollten.

Handhabung, Anpassungsfähigkeit & Skalierbarkeit

Wie gut lässt sich die Lösung in Ihr Unternehmen integrieren?

Achten Sie darauf, dass sich die Lösung Ihren Anforderungen anpasst – und nicht andersherum.

Nutzer-, Rechte- oder auch Geräteverwaltung. Handhabung durch verschiedene Mitarbeiter. Kompatibilität mit verschiedenen Endgeräten. All diese Aspekte verlangen nach einer höchst anpassungsfähigen und skalierbaren IIoT-Lösung.
Achten Sie deshalb bei der Suche und Auswahl Ihrer IIoT-Service-Plattform, dass diese sich Ihren Bedürfnissen anpassen lässt und vermeiden Sie unflexible Produkte, nach denen Sie Ihre Prozesse und Ihre Strukturen ausrichten müssten.

Intuitive Handhabung
Damit Sie Themen wie die Nutzer-, Rechte- oder auch Geräteverwaltung möglichst effizient bearbeiten können, ist es ratsam mit einer Lösung zu arbeiten, die über klare Strukturen verfügt und intuitiv zu bedienen ist. So verlieren Sie keine Zeit, wenn Sie bspw. Servicemitarbeitern Zugriffsrechte auf bestimmte Maschinen gewähren oder wenn Sie Servicemitarbeitern konkrete Servicefälle zuweisen.

No-Code-Plattform
Ein wesentlicher Aspekt in diesem Zusammenhang ist das Thema Webinterface. Hier sollten Sie auf eine sogenannte No-Code-Plattform zurückgreifen, für deren Bedienung keine speziellen IT-Kenntnisse, sprich Programmierkenntnisse notwendig sind. So können Sie auch anspruchsvolle IIoT-Anwendungen realisieren, wie z. B. das Auslesen und Visualisieren von Grafiken von Maschinen-/Anlagenzuständen und brauchen keinen Spezialisten zu Rate ziehen.

Anpassungsfähige Lösung
Eine anpassungsfähige Lösung erkennen Sie z. B. daran, dass sich der Anbieter nicht auf eine spezielle Branche oder ein bestimmtes Endgerät fokussiert und seine Lösung auch mit dem Betriebssystem funktioniert, welches derzeit in Ihrem Unternehmen eingesetzt wird und Sie nicht erst ein neues Betriebssystem zu installieren brauchen.

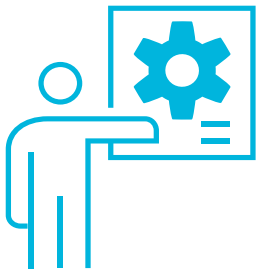
Bedarfsorientierte Skalierbarkeit
Da sich im Laufe der Nutzungszeit eventuell auch Ihr Bedarf hinsichtlich der wartungsbedürftigen Maschinenanzahl verändern könnte, sollte Ihre IIoT-Lösung sowohl auf ganz wenige als auch eine Vielzahl von Maschinen ausgelegt sein.

Tipp: Um sicher zu gehen, dass die gewählte IIoT-Lösung auch wirklich anpassungsfähig ist, lassen Sie sich vom Anbieter passende Referenzprojekte mit vergleichbaren Rahmenbedingungen zeigen.

Fazit

Je klarer Sie im Vorfeld Ihre Anforderungen definieren, desto leichter wird Ihnen die Entscheidung am Ende fallen.

Die Unternehmens- und Strategieberatung McKinsey & Company schätzt, dass deutsche Unternehmen bis 2025 durch konsequente Digitalisierung, zu denen auch die Themen Fernwartung und IIoT gehören, 126 Milliarden Euro zusätzlich an Wertschöpfung erzielen können[4]. So wundert es wenig, dass derzeit viele Unternehmen aktiv nach einer Lösung Ausschau halten. Die in diesem Whitepaper beleuchteten Auswahlkriterien stellen aus unserer Sicht eine gute Orientierungshilfe bei der Auswahl der passenden IIoT-Lösung dar. Die finale Entscheidung darüber, welche IIoT-Lösung nun die Beste für Sie und Ihr Unternehmen ist, hängt also maßgeblich davon ab, wie gut Sie Ihre Anforderungen – wenn möglich, auch direkt mit dem Anbieter im Rahmen eines Workshops o. ä. – im Vorfeld definieren.



Wichtig: Überstürzen Sie Ihre Entscheidung nicht. Lassen Sie sich Zeit und implementieren Sie in Ihrem Unternehmen nur eine Lösung, die Sie auf Herz und Nieren überprüft haben und von der Sie auch wirklich überzeugt sind.

Sollten Sie am Ende Ihrer Recherche mehrere Anbieter im Visier haben, kann es hilfreich sein, sich die Lösung vorführen zu lassen. Einige Anbieter bieten Seminare oder Online-Demos an. Registrieren Sie sich, lassen Sie sich die Lösung erläutern, stellen Sie Fragen und fühlen Sie dem Anbieter auf den Zahn. Dies kann Ihnen ein Gefühl vermitteln, ob die Lösung dem entspricht, was Sie sich vorgestellt haben.

Sollten dann für Sie immer noch mehrere Anbieter in Frage kommen, empfiehlt es sich, die ausgewählten Lösungen einfach mal unverbindlich zu testen. Einige Anbieter stellen eigens hierfür Testzugänge bereit oder versenden Testgeräte, die Sie in Ihrem Unternehmen von Ihrem gesamten Team testen lassen können.

Checkliste

Checkliste für die Auswahl einer passenden Industrial-IoT-Lösung
Die nachfolgende Checkliste enthält die aus unserer Sicht wichtigsten Aspekte, die Sie bei der Suche und Auswahl einer IIoT-Lösung berücksichtigen sollten. Können Sie alle folgenden Punkte erfolgreich abhaken, handelt es sich bei Ihrer Auswahl mit höchster Wahrscheinlichkeit um eine moderne, sichere und anpassungsfähige IIoT-Lösung.

Verbindungsaufbau

Ist gewährleistet, dass Verbindungen ausschließlich von innen nach außen aufgebaut werden können?

Fernwartungszugriff

Besteht während des Zugriffs eine verschlüsselte Verbindung zwischen Dienstleister und Maschinenbetreiber?

Datentransfer

Werden die vom BSI empfohlenen Verschlüsselungs-Standards verwendet?

Identifizierung

Ist eine eindeutige Identifizierung über Smartcards oder ein Hardwarezertifikat auf einem Crypto-Chip gewährleistet?

2-Faktor-Authentifizierung

Erfolgt die Passwort-Authentifizierung über eine gängige Authenticator App und/oder E-Mail?

Rechteverwaltung

Lassen sich benutzerdefinierte Gruppen/Organisationen erstellen und mit spezifischen Rechten auszeichnen?

Nachrichtenerfassung

Lässt sich jede Verbindung inkl. Informationen zum Besucher und Dauer eindeutig erfassen und zuweisen?

Verschlüsselung

Werden sichere kryptische Verschlüsselungs-verfahren nach aktuellen Empfehlungen des BSI eingesetzt?

No-Code-Plattform

Ist die Möglichkeit der einfachen Erstel-lung von Visualisierungen ohne spezielle Programmierkenntnisse gegeben?

Anpassungsfähigkeit

Lässt sich die Lösung an vorhandene Betriebssysteme und Endgeräte beim Kunden anpassen?

Bei Fragen wenden Sie sich bitte ads-tec Industrial IT GmbH:
Tel.: +49 70 22 25 22-200 E-Mail: sales@ads-tec.de

Quellen

1 Lichtblau, K.; Schleiermacher, T.; Goecke, H.; Schützdeller, P.

Digitalisierung der KMU in Deutschland. Konzeption und empirische Befunde. 2018.

URL: https://www.iwconsult.de/fileadmin/user_upload/projekte/2018/Digital_Atlas/Digitalisierung_von_KMU.pdf (Stand: 19.11.2020)

Original Zitat aus: Raphael Kiesel, Timo Heutmann, Jan Dering, Alexander Kies, Thomas Vollmer, Robert H. Schmitt
Whitepaper Cybersecurity in der vernetzten Produktion. 2020.

URL: https://www.ipt.fraunhofer.de/content/dam/ipt/de/documents/whitepaper/whitepaper-cybersecurity-in-der-vernetzten-produktion.pdf

2 Checkpoint Software Technologies

Umfrage zum Status der IT-Sicherheit nach der Corona-Hochphase. 2020.

URL: https://www.infopoint-security.de/check-point-umfrage-zum-status-der-it-sicherheitnach-der-corona-hochphase/a24059/

3 BSI-Veröffentlichung zur Cyber-Sicherheit

Fernwartung im industriellen Umfeld. 2018.

URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_108.pdf;jsessionid=6A09424BCC4D7BFC46FC7D9B4E959FCE.internet082?__blob=publicationFile&v=1 (Stand: 11.07.2018)

4 McKinsey & Company (Hrsg.)

Digitalisierung im Mittelstand erhöht Wachstum in Deutschland um 0,3 Prozentpunkte pro Jahr. 2017.

URL: https://www.mckinsey.com/de/news/presse/di%ADgitalisierung-im-mittelstand-erhoht-wachstum-in-deutschland-um-03-prozentpunkte-pro-jahr (Stand: 15.01.2019)

Original Zitat aus: Raphael Kiesel, Timo Heutmann, Jan Dering, Alexander Kies, Thomas Vollmer, Robert H. Schmitt
Whitepaper Cybersecurity in der vernetzten Produktion. 2020.

URL: https://www.ipt.fraunhofer.de/content/dam/ipt/de/documents/whitepaper/whitepaper-cybersecurity-in-der-vernetzten-produktion.pdf

ads-tec Industrial IT GmbH
Heinrich-Hertz-Straße 1
D-72622 Nürtingen
Telefon +49 70 22 25 22-200
Telefax +49 70 22 25 22-402
sales@ads-tec.de
www.ads-tec.de