Internet of Things

Mit Sicherheit zum Erfolg

Einfach ist die Umsetzung von Internet-of-Things-Projekten (IoT) nicht. Oft stehen Sicherheitsbedenken im Weg. Zwei IoT-Experten haben vier goldene Regeln aufgestellt, die sicher zum Ziel führen.

Wie ein roter Faden zieht sich der Sicherheitsaspekt durch sämtliche IoT-Projekte. Aufgrund der rasanten Zunahme von Vernetzungsmöglichkeiten werden immer mehr Daten gesammelt, die nutzbringend für den Kunden eingesetzt werden. Dies geschieht beim Vernetzen von Prozessen, Produkten und Dienstleistungen mit Kunden und auch Firmen. Der Cyber Kriminalität werden dadurch viele Türen geöffnet.

Die folgenden vier Regeln inklusive Sicherheitstipps helfen Ihnen, Ihr Projekt sicher zum Erfolg zu führen:

WEB-TIPP:
www.zuehlke.com

1

IoT-Regel Nummer 1:
New Business statt Daily Business

Um neue Geschäftsideen zu finden, ist es wichtig, sich vom Daily Business loszulösen. Digitalisierungsinitiativen beziehungsweise IoT-Projekte benötigen Raum für Kreativität und Interdisziplinarität. Auch sollte eine Fehlerkultur erlaubt werden, die die Flexibilität zum Lernen zulässt und es ermöglicht, getroffene Annahmen und Anforderungen zu ändern. Die Flexibilität wird ebenfalls benötigt, um auf Erkenntnisse aus neuen Regulierungen, Standard- oder Technologieänderungen agil reagieren zu können.

„Als Kundin ist es mir wichtig zu wissen, wofür meine Daten verwendet werden. Daher bevorzuge ich Firmen, die nach dem Prinzip «Die Daten gehören dem Kunden» vorgehen."

Rahel Weber,
Lead Consultant bei Zühlke

Eine Abtrennung der IoT-Initiativen vom Daily Business gibt Raum für strukturelle und kulturelle Änderungen, ohne dabei das bestehende Geschäft einzuschränken. Durch den Einsatz von Innovationstechniken, kombiniert mit dem Wissen, was mit dem Internet der Dinge alles möglich ist, wird es gelingen, neue Businessmodelle zu definieren und neue Ertragsquellen zu entdecken.

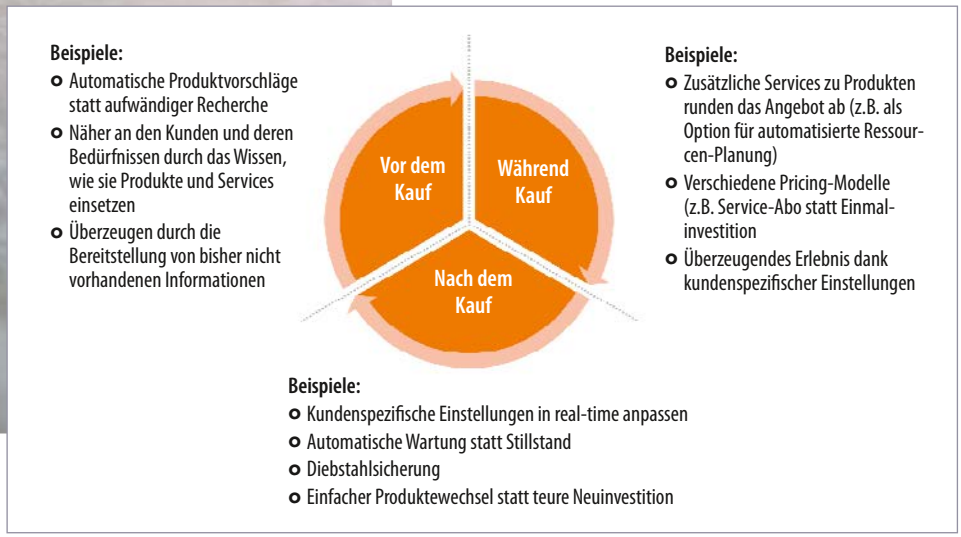
2

IoT-Regel Nummer 2:
Kunden, nicht Prozesse!

IoT wird vorausgesagt, dass es den Produktemarkt signifikant beeinflussen wird. Die Tatsache, dass zusätzliche Dienstleistungen zu physischen Produkten angeboten werden und dass Informationen benutzergerecht zum richtigen Zeitpunkt zur Verfügung gestellt werden, öffnet neue Türen und Gestaltungsraum für Kundenerlebnisse. Wenn es jedoch um Kundendaten geht, stellt sich zuerst die Frage: Was genau ist der Kundennutzen, wenn ich diese Daten sammle und einsetze? Klar ist: Wenn der Nutzen groß ist, sind Kunden bereit, Informationen preiszugeben. Entscheidend ist, wie heikel die Kundendaten sind und wie man die Sicherheit gewährleisten kann, ohne das Kundenerlebnis spürbar einzuschränken. Generieren Sie Kundennutzen, rechnen sich auch Investitionen in die Sicherheit. Um das Vertrauen gegenüber dem Kunden zu ge-

an einen Gerätehersteller, der Diebstahlschutzfunktionen mit Real-Time-Alarm über das Handy anbietet. Könnte da nicht je nach Gerät plötzlich eine Partnerschaft mit einer Versicherung interessant werden?

Die zentralen Fragen bei der Wahl der richtigen Partner liegen auf der Hand: Welche Elemente der Wertschöpfung können vom Partner übernommen werden und welche müssen in-house bleiben? Wo soll mich meine Vision und Strategie in der Welt der Digitalisierung hinführen? Welches sind meine heutigen Kernkompetenzen? Welche Kernkompetenzen müsste man aufgrund der Digitalisierung bzw. den Möglichkeiten von IoT auf- oder ausbauen? Was geschieht in meinem Umfeld und wie schnell muss ich reagieren? Die Antworten auf diese Fragen bilden die Grundlage für die Entscheidung, wann auf interne und wann auf externe Ressourcen zurückgegriffen werden soll.



Echter Kundennutzen, ermöglicht durch IoT.

winnen, gilt es, nach dem Prinzip «Die Daten gehören dem Kunden» vorzugehen. Dies schafft volle Transparenz gegenüber dem Kunden und gibt ihm die Möglichkeit, sich auf seinen Wunsch vom Angebot zurückzuziehen.

Mit der Gestaltung des Kundenerlebnisses können Sie wie folgt starten: Wählen Sie Produkte und Dienstleistung aus dem aktuellen Portfolio, deren Wirkungsfeld Sie bezüglich Kundenerlebnis herausfordern möchten. Ziehen Sie neu auch die Möglichkeiten der Digitalisierung in Betracht. Versetzen Sie sich in den Benutzer dieser Geräte und versuchen Sie, Antworten auf folgende Fragen zu finden: Wie würden die sogenannten Digital Natives mit diesem Produkt oder Service umgehen? Könnten spielerische Elemente wie Social Media, digitale Applikationen, etc. einen Mehrwert beim Kundenerlebnis bieten? Seien Sie kreativ und fragen Sie auch die erwähnte Generation – zum Beispiel die Lehrlinge in Ihrem Betrieb.

Weitere wichtige Fragen wären: Welche Produkte oder Services – beispielsweise zusätzliche Informationen – würden das Kundenerlebnis abrunden? Wollen Sie dies in Zukunft selbst anbieten oder wäre ein strategischer Partner eine Option? Wie bieten Unternehmen aus anderen Branchen einzigartige Kundenerlebnisse an? Gerade beim Thema Internet of Things lohnt es sich, Ideen aus völlig unterschiedlichen Bereichen zu holen.

3

IoT-Regel Nummer 3: Die richtigen Partner

Die Vielfalt und Wichtigkeit von neuen Business-Partnern im IoT-Ökosystem ist nicht zu unterschätzen. Denn genau diese wird es durch die großen Veränderungen im Markt und das Näheraneinanderrücken von verschiedenen Branchen bei IoT-Lösungen brauchen. Denken Sie

Wegen der zunehmenden Vernetzungsmöglichkeiten verlangen gute IoT-Lösungen mehr Offenheit im Austausch von Informationen zwischen Partnern, als dies heute im Business üblich ist. Transparenz braucht Mut. Fragen müssen geklärt werden: Wer hat wann Zugriff auf welche Daten? Und wer braucht die Informationen überhaupt? Welche Kommunikation muss über die kritische Infrastruktur und Kontrolleinheit laufen? Stellt man die Transparenz sicher, lässt sich die Sicherheit automatisch erhöhen.

Die Sicherheit in Bezug auf die menschlichen Zugriffe – sowohl auf Kunden- wie auch auf Partnerseite – darf ebenso nicht vernachlässigt werden. Wie lässt sich verhindern, dass ein Unbefugter die Steuerung meiner Maschinen übernimmt? Hier gilt für IoT, was in anderen Bereichen wie dem Online-Banking schon seit langem üblich ist: Sobald der Mensch eingreift, braucht es eine starke Authentifizierung anhand von zwei oder mehr Faktoren. Zudem sollte das System Manipulationen erkennen – insbesondere bei physischem Zugriff durch den Endbenutzer. Prinzipien, die sich in den letzten Jahrzehnten bezüglich Sicherheit bei Software und Webtechnologien durchgesetzt haben sowie Ansätze rund um die Sicherheit in der Operation Technology (OT) sollten bei IoT-Anwendungen berücksichtigt werden.

4

IoT-Regel Nummer 4: Step-by-Step statt Grossprojekt

Firmen, die bereits IoT-Initiativen lanciert haben, geben als wichtigste «Lesson Learned» an: klein starten und Schritt für Schritt vorwärtsgehen. Die Erfahrung auch mit herkömmlichen IT- und Entwicklungsprojekten zeigt, dass mit kleinen Schritten immer die größten Erfolge erzielt werden.

Um dem digitalen Alptraum zu entkommen, dass neue Unternehmen die Branche revolutionieren, braucht es Weitblick, innovative Ideen und ein flexibles Organisationsmodell. Vergessen Sie nicht, dass Sie in Ihrem Unternehmen bereits auf sehr viel Bestehendem aufbauen können. Dies gilt es zu analysieren, um die anstehende digitale Transformation richtig in Ihrem Unternehmen aufzuhängen.

„Um dem digitalen Alptraum zu entkommen, dass neue Unternehmen die Branche revolutionieren, braucht es Weitblick, innovative Ideen und ein flexibles Organisationsmodell."

Hansjürg Inniger,
Director Solution Center Internet of Things & Partner bei Zühlke

Starten Sie kein Großprojekt. Leiten Sie aus Ihrer Vision kleinere Teilziele ab, die Sie Schritt für Schritt umsetzen. So können Sie den Reifegrad Ihrer IoT-Angebote kontinuierlich erhöhen. Am besten definieren Sie jeden Schritt bzw. jedes Teilziel als Minimum Viable Product. Auf diese Weise können Sie Ihre Idee bzw. Ihr Produkt bereits sehr früh am Markt testen. Welche Vorteile schaffen Sie sich dadurch? Nebst dem direkten Feedback vom Markt lernen Sie mit jedem Schritt dazu. Sie werden schneller, die Risiken geringer und die Kosten können über die Zeit verteilt werden. Ist Ihre Innovation nicht erfolgreich, gilt: «fail fast, but cheaply». Der Schritt-für-Schritt-Ansatz hilft Ihnen auch, neue Erkenntnisse oder Änderungen im Entwicklungsprozess schnell zu adressieren. Sicherheitsfragen gilt es in der Business Analyse, im Requirements Engineering sowie in der Architektur von Anfang an zu berücksichtigen – dies bezieht sich nicht nur auf IT-, sondern auch auf OT-Fragen.

Sie wollen beim Go-Live keine Überraschung erleben. Adressieren Sie deshalb folgende Sicherheitsthemen von Anfang an und kontinuierlich übers Projekt hinweg:

- Identifizieren Sie die Daten mit hohem Kundennutzen und mit heiklem Informationsgehalt sowie kritische vernetzte Infrastrukturen und deren Kontrollnetzwerke.
- Schaffen Sie Transparenz in Bezug auf wer, wann, auf welche Daten zugreift und wer diese Informationen auch wirklich braucht. Klären Sie ab, welche Kommunikation wirklich für den Betrieb Ihrer Kontrollnetzwerke und vernetzten Infrastrukturen benötigt wird.
- Sorgen Sie für eine sichere Verschlüsselung der Datenströme – egal, ob von Maschine zu Maschine, vom End-User zur Maschine oder von den Geräten zum Server in der Cloud.
- Erstellen Sie Prozeduren für Maßnahmen bei Hackeingriffen (Business- und IT-seitig), um eine schnelle Reaktionszeit zu gewährleisten.

Da die ganze Organisation durch IoT betroffen ist, sind eine breite Kommunikation und gute Kommunikationsstrategien unabdingbar. Am besten verwendet man so früh wie möglich eine Visualisierung der IoT-Vision und -Mission. Diese erlaubt es den involvierten Personen (IT, R&D und business-relevanten Disziplinen sowie auch Kunden oder Vertreter aus anderen Branchen), Fragen zu stellen und Anforderungen zu formulieren, an die man sonst nicht gedacht hätte.

Zögern Sie noch immer, trotz der goldenen vier IoT-Regeln, Ihre digitalen bzw. IoT-Initiativen zu starten?

Sicherheitsthemen im IoT-Bereich sind lösbar. Dies zeigen zwei Beispiele aus der Praxis. Zühlke begleitete zwei Kunden aus der Sicherheitsbranche bei IoT-Vorhaben: dorma+kaba, eine Anbieterin von Sicherheits- und Zutrittslösung, bei ihrem vernetztes Schließsystem, und Securiton, ein Hersteller von Alarm- und Brandmeldesystemen.

Rahel Weber, Hansjürg Inniger

Weiterführende Informationen: www.it-daily.net

Blog

Der Button führt Sie in der ePaper-Version direkt zum Ziel. In der Printversion nutzen Sie bitte den QR Code.