Privatsphäre macht den Unterschied

Schon in 10 bis 15 Jahren soll es laut aktuellen Vorhersagen weltweit 50 Milliarden vernetzte Geräte geben. Damit wird auch die Menge der personenbezogenen Daten, die durch vernetzte Devices tagtäglich gesammelt werden, drastisch ansteigen.

Mit den zahlreichen neuen Möglichkeiten, die das Internet der Dinge bietet, wachsen auch die Sicherheitsrisiken rasant. Die Kontrolle über die Daten geht zum Teil verloren – Datenskandale sind schon fast an der Tagesordnung. So stand bspw. die Gesundheitsapp Ada aufgrund massiver Datenschutzmängel in der Kritik, oder als sich Ende 2019 ein Hacker über Smart-Home-Produkte Zugang zu zahlreichen persönlichen Daten verschafft hatte. Nicht zu vergessen der Fall Cambridge Analytica bei dem Nutzerdaten für den Wahlkampf missbraucht wurden.

Es stehen daher nicht nur die Technologie von Smart Ecosystems, also Systemen, die Menschen, digitale Systeme und Objekte aus der realen Welt verknüpfen, auf dem Prüfstand, sondern auch der sorglose Umgang mit den gesammelten Daten bzw. die Einhaltung der Privatsphäre.

Die beiden Kernfaktoren Transparenz und Kontrolle spielen für den Endnutzer beim Thema Privatsphäre die wichtigste Rolle. Wir empfehlen, diese beiden Bereiche unbedingt in Ihren Smart Ecosystems zu berücksichtigen:

Transparenz	Kontrolle
Informieren Sie den Verbraucher, welche persönlichen Daten erfasst werden – und zwar nicht im Vorfeld durch zahlreiche Seiten Kleingedrucktes. Informieren Sie Kunden am besten genau zu dem Zeitpunkt, bei dem es innerhalb des IoT-Produkts zu einer Datenerfassung kommt. Kommunizieren Sie dabei so einfach und verständlich wie möglich. Stellen Sie heraus, welchen Vorteil Ihre Kunden durch die Datenerfassung haben und wozu Sie als Unternehmen diese Daten verwenden	Legen Sie die Entscheidung in die Hände der Verbraucher, welche Daten Sie als Unternehmen verwenden dürfen. Achten Sie dabei auch wieder auf den richtigen Zeitpunkt der Entscheidung. Lassen Sie den Verbrauchern wieder genau dann die Wahl, wenn Ihr Produkt relevante Daten speichern möchte

Ebenfalls halten wir die folgenden vier Tipps für relevant:

1. Stellen Sie die Privatsphäre des Kunden bei Ihren Produkten immer in den Mittelpunkt.

2. Vermeiden Sie es, lediglich den Mindeststandard von Sicherheitsrichtlinien zu erfüllen. Dies reicht lange nicht aus und führt dazu, dass vernetzte Geräte entwickelt werden, die gerade einmal nur gut genug für den Schutz der Privatsphäre sind.

3. Machen Sie das Thema Privatsphäre zum Alleinstellungsmerkmal Ihrer vernetzten Geräte und nutzen Sie diese Message für Marketing und Kommunikation – so verschaffen Sie sich einen echten Wettbewerbsvorteil.

4. Rechtlich konform zu sein resultiert oft in langen und unverständlichen Texten. Entwickeln Sie ein Verständnis für die Kunden, wenn Sie sie über das Thema Sicherheit informieren. Gestalten Sie Ihre Kommunikation verständlich und übersichtlich, sodass Informationen nicht als lästig betrachtet werden.

BEISPIELBEREICHE FÜR IOT-ANWENDUNGEN

PHARMA & CHEMIE

- Verfahrenstechnik
- Cloudshift und Sicherheit
- Reduzierung des Energieverbrauchs
- Echtzeit-Compliance
- Reduzierter Rechercheaufwand
- Mobiler Kontrollraum

FINANZEN & BANKWESEN

- Mobile Bezahlung, POS, ATM
- Intelligente Plattformen
- Verbindung von Filial- und Einzelhandel
- Echtzeitverarbeitung
- Machine Learning und Robo-Advisors
- Integration von Wearables