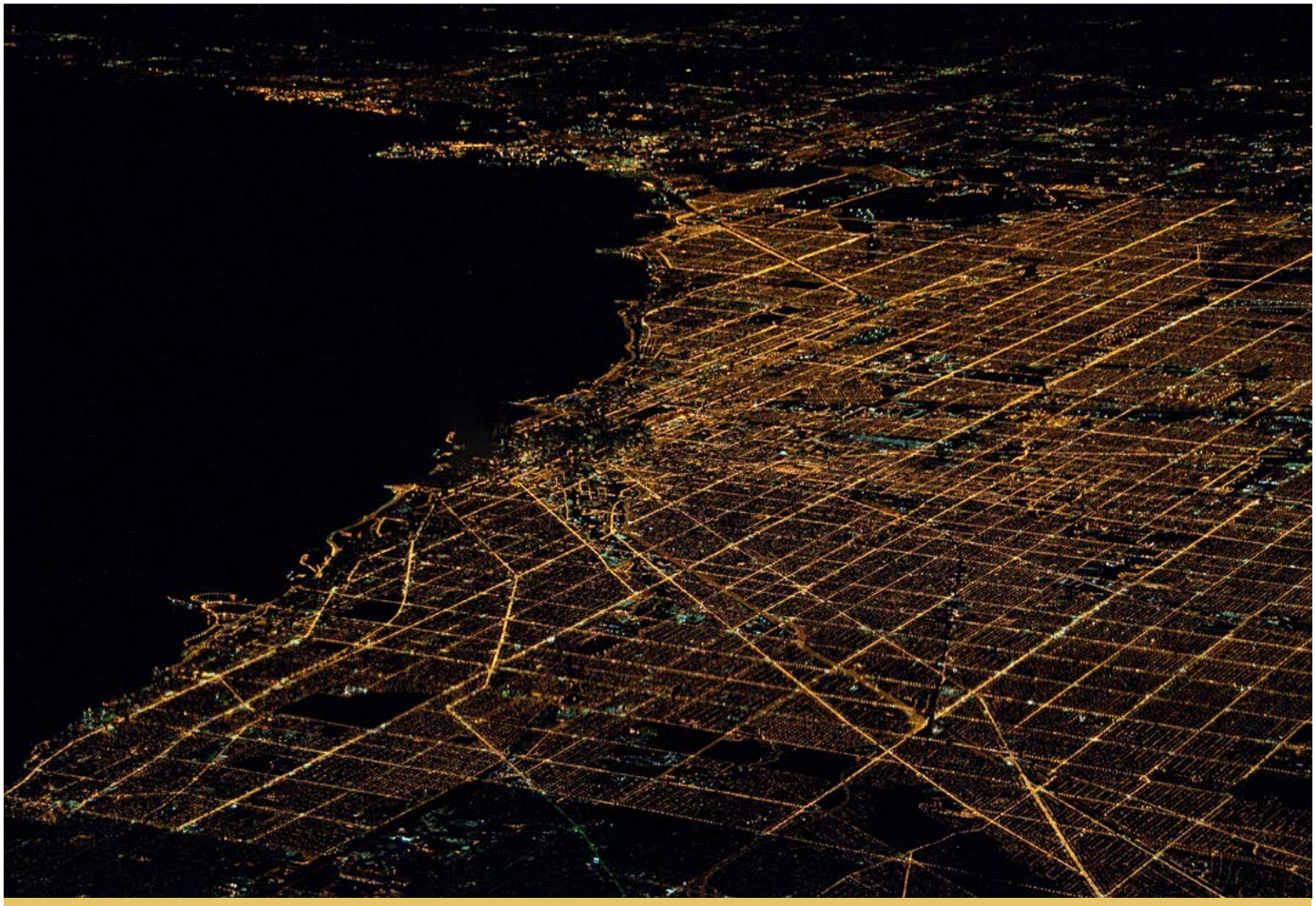


IoT, aber bitte mit Security

Fachartikel
Urs Zurbuchen, lic. oec. publ.
Senior Security Consultant, Ergon Informatik AG
Benedikt Ostermaier, Dr. sc. ETH Zürich
Head of IoT, Ergon Informatik AG

Erschienen im Ergon Magazin 2019
SMART insights

ergon

Ob Zahnbürste, Heizung, Auto oder Industrieanlage – mehr und mehr Dinge unseres Alltags werden vernetzt, sei es lokal oder über das Internet. Sie kommunizieren nicht nur miteinander, sondern auch mit Smartphone-Apps, Cloud-Anwendungen und (Mehrwert-)Diensten des Herstellers oder Dritter. Dadurch lassen sich beispielsweise neue Anwendungsfälle umsetzen, Prozesse effizienter gestalten oder neue Geschäftsmodelle realisieren. Führt man den Vernetzungsgedanken konsequent zu Ende, entstehen ganze IoT-Ökosysteme, deren Mehrwert sich im Zusammenspiel aller Komponenten ergibt. Auf technischer und organisatorischer Ebene kann dabei von starken Synergieeffekten profitiert werden. Welche das sind, erklären IoT-Profi Benedikt Ostermaier und Security-Experte Urs Zurbuchen.

Neben den vielen positiven Effekten bieten die zahlreichen Kommunikationsschnittstellen der einzelnen Systembausteine böswilligen Zeitgenossen auch neue Angriffsflächen. Für den Hersteller von IoT-Geräten ist es überlebenswichtig, nicht durch Nachlässigkeit oder frühere Fehlentscheide den guten Ruf zu verlieren. Im Internet of Things muss die IT-Security daher ein integraler Bestandteil sein und darf nicht nur auf die einzelnen Geräte beschränkt werden. Stattdessen ist das Thema systemübergreifend zu betrachten.

Die digitale Geburt

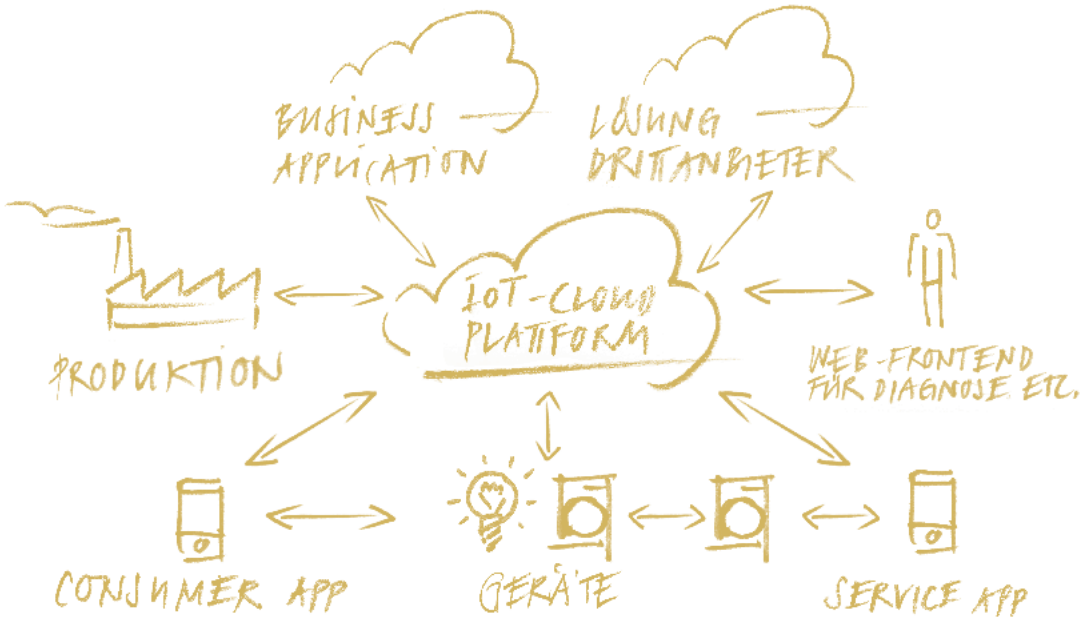
Der digitale Lebenszyklus eines IoT-Geräts beginnt bei seiner Produktion: Hier erhält es eine sichere Identität (in Form eines Schlüsselpaares/Zertifikats) und wird ggf. digital «versiegelt». Dieser sensible Prozess muss unbedingt gewährleisten, dass nur Berechtigte Geräte erzeugen und keine Duplikate entstehen. Die sichere Identität wird verwendet, um sich später gegenüber anderen Komponenten digital auszuweisen, und bietet somit die Grundlage für eine gesicherte Zusammenarbeit mit anderen Bausteinen des IoT-Ökosystems.

Dreh- und Angelpunkt in der Cloud

Als zentrale Kommunikationsdrehscheibe und Vermittler agiert oftmals eine IoT-Cloud-Plattform, die Basisfunktionen für Betrieb, Integration und Sicherheit anbietet. Bei der Produktion eines Geräts wird es in der IoT-Cloud-Plattform mit seinem digitalen Geburtsschein bekannt gemacht. Anschliessend kann das Gerät mit der Plattform über eine abgesicherte Verbindung kommunizieren. Dort existiert das Gerät in Form eines digitalen Zwillings, der als Stellvertreter für das physische Gerät die einheitliche Einbindung in Business-Applikationen ermöglicht. Punkto Sicherheit kommt der IoT-Cloud-Plattform eine zentrale Rolle zu: Sie beschränkt den Zugriff auf berechtigte Personen bzw. Applikationen, überwacht die Geräte im Feld und ermöglicht deren Aktualisierung mittels Firmware-Updates. Die Sicherheitsanforderungen an diese Plattform sind daher entsprechend hoch.

IoT-Geräte: keine Blösse bieten

Die Geräte im Feld kommunizieren typischerweise über eine sichere Verbindung mit einer IoT-Cloud-Plattform. Zugriffsberechtigungen werden in diesem Fall von der Plattform verwaltet und durchgesetzt. Im Falle einer lokalen Kommunikation, wie z.B. im Servicefall, muss das Gerät etwaige Berechtigungen selbst überprüfen. Ein besonderer Fall ist die «digitale Inbesitznahme»: Hier weist der Nutzer das Gerät selbst seinem Account zu, um anschliessend remote darauf zugreifen zu können. Dazu muss er üblicherweise demonstrieren, dass er physischen Zugriff zum entsprechenden Gerät hat, indem er z.B. während eines Zeitfensters eine bestimmte Aktion am Gerät durchführt.



«Der digitale Lebenszyklus eines IoT-Geräts beginnt bei seiner Produktion: Hier erhält es eine sichere Identität und wird ggf. digital versiegelt.»

Darüber hinaus müssen IoT-Geräte unbedingt die Möglichkeit besitzen, ihre Firmware über die Cloud zu aktualisieren. Nur so können neu entdeckte Sicherheitslücken rasch und effizient behoben werden. Zudem verfügen IoT-Geräte oft nur über begrenzte Ressourcen, was die Nutzung von Security-Mechanismen erschweren kann.

.

Das Smartphone als Dompteur der Dinge

Viele IoT-Geräte bieten dem Anwender die Möglichkeit, sie mit einer Smartphone-App zu konfigurieren und anzusteuern. Diese Kommunikation verwendet Standardprotokolle (z.B. REST/JSON via HTTP) und ist deshalb nicht auf die App beschränkt, sondern kann auch anderweitig ausgelöst werden. Entsprechend wichtig, aber auch schwierig ist die Zugriffskontrolle, damit nur Berechtigte zugelassen werden. Kurzsichtig wäre z.B. ein Ansatz, die App mit einem geheimen Berechtigungsschlüssel auszustatten. Es existieren nämlich verschiedene Decodiermechanismen, so dass das Geheimnis nicht lange eines bleibt. Ähnlich, aber sogar noch diffiziler gestaltet sich die Situation für Zugriffe im Servicefall. Während bislang dedizierte Servicegeräte genutzt wurden, die über proprietäre Schnittstellen mit den Geräten kommunizierten, kommen zukünftig Service-Apps zum Einsatz. Diese können auf Bereiche und Funktionen zugreifen, die üblicherweise dem Anwender nicht zur Verfügung stehen sollen.

«Im Internet of Things muss die IT-Security ein integraler Bestandteil sein und darf nicht nur auf die einzelnen Geräte beschränkt werden.»

Integrativer Ansatz sichert Erfolge

Für Gerätehersteller als auch Lösungsanbieter und Unternehmen, die IoT-Lösungen einsetzen, bietet das Internet der Dinge effiziente und begeisternde Möglichkeiten. Entsprechend hoch ist die Innovationsrate und damit der Druck, verschiedenste Komponenten und Dienste in das Ökosystem zu integrieren. Daraus entsteht ein heterogenes und komplexes Gebilde. Die Herausforderung, dieses sicher umzusetzen, darf nicht unterschätzt werden. Die Verantwortung liegt einerseits beim IoT-Geräte-Anbieter, der die vielen Security-Aspekte als integralen Bestandteil seines Angebots betrachten und von Beginn weg berücksichtigen sollte. Andererseits müssen Unternehmen, die IoT-Lösungen einsetzen, sicherstellen, dass die notwendigen Security-Massnahmen ergriffen wurden.

Urs Zurbuchen, lic. oec. publ.
Senior Security Consultant
urs.zurbuchen@ergon.ch

Benedikt Ostermaier, Dr. sc. ETH Zürich
Head of IoT
benedikt.ostermaier@ergon.ch