eBOOK
www.ip-insider.de

IP Insider

IoT und Industrie 4.0

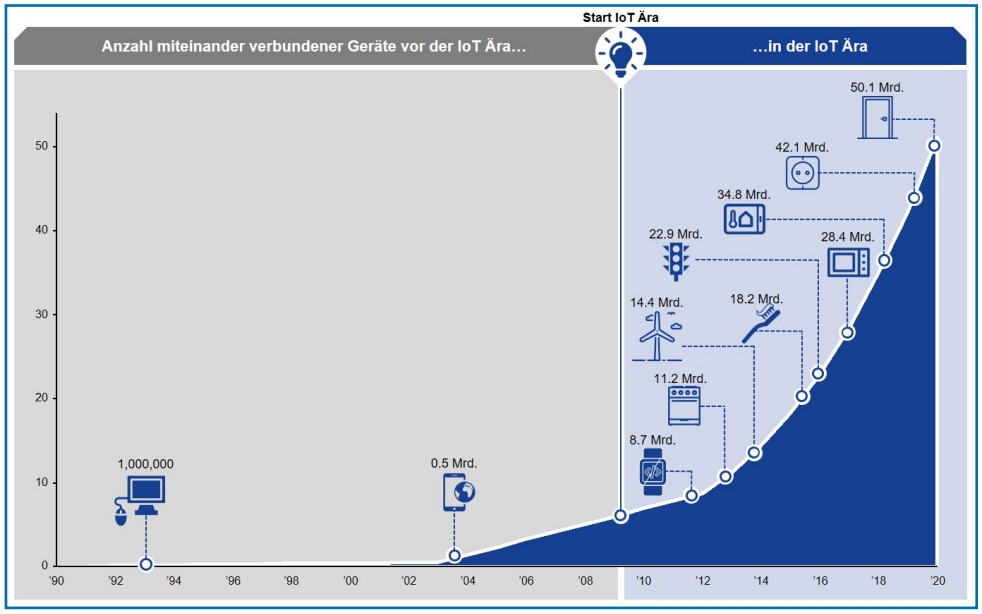
Auf dem Weg zur Massenkommunikation
Sicherheit als allgemeines IoT-Problem
Warum moderne Industrie ohne IoT undenkbar ist

Inhalt

Vogel IT-Medien GmbH
Max-Josef-Metzger-Str. 21
86157 Augsburg
Telefon +49 (0) 821/2177-0
E-Mail redaktion@ip-insider.de
Web www.IP-Insider.de
Geschäftsführer: Werner Nieberle
Chefredakteur: Andreas Donner, V.i.S.d.P.,
andreas.donner@vogel-it.de
Erscheinungstermin: April 2019
Titel: phonlamaiphoto/stock.adobe.com

Auf dem Weg zur Massenkommunikation

Kaum eine Presse- oder Unternehmensmeldung aus dem Umfeld der IT kommt heute ohne die Begriffe IoT und Industrie 4.0 aus. 1999 – so will es die IT-Historie – soll der Begriff vom „Internet der Dinge“ erstmals aufgetaucht sein. Wie sieht es mit diesen Techniken heute, im Jahr 2019 aus? Wir grenzen ab: Was ist (immer) noch Hype und was ist jetzt schon Realität?



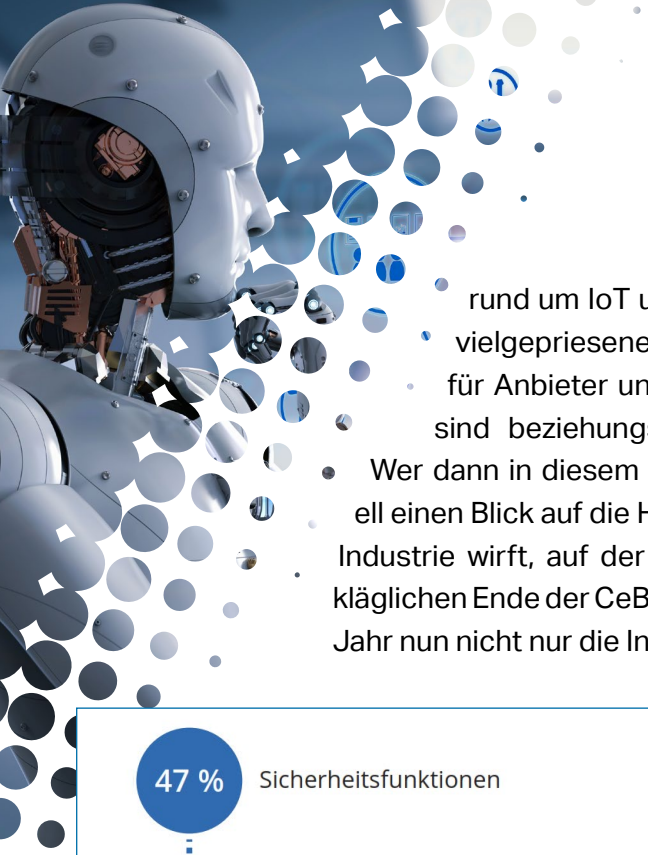
Die Spezialisten des Strategieberatungs-Unternehmens Fostec & Company haben einen Blick auf die Zeit vor und nach der Einführung von IoT gewagt: Dabei stellten sie fest, dass bereits in den letzten Jahren eine explosionsartige Entwicklung der vernetzten Dinge stattgefunden hat. (Bild: Fostec & Company)

Glaubt man den Berichten (und auch den Wikipedia-Einträgen), so war es wohl der Brite Kevin Ashton, der im Jahr 1999 den Begriff „Internet of Things“ erstmals nutzte. Er arbeitete damals beim Unternehmen Proctor & Gamble und befasste sich mit der zu diesem Zeitpunkt noch recht innovativen RFID-Technik, die helfen sollte, die Supply-Chain des Unternehmens besser zu verwalten.

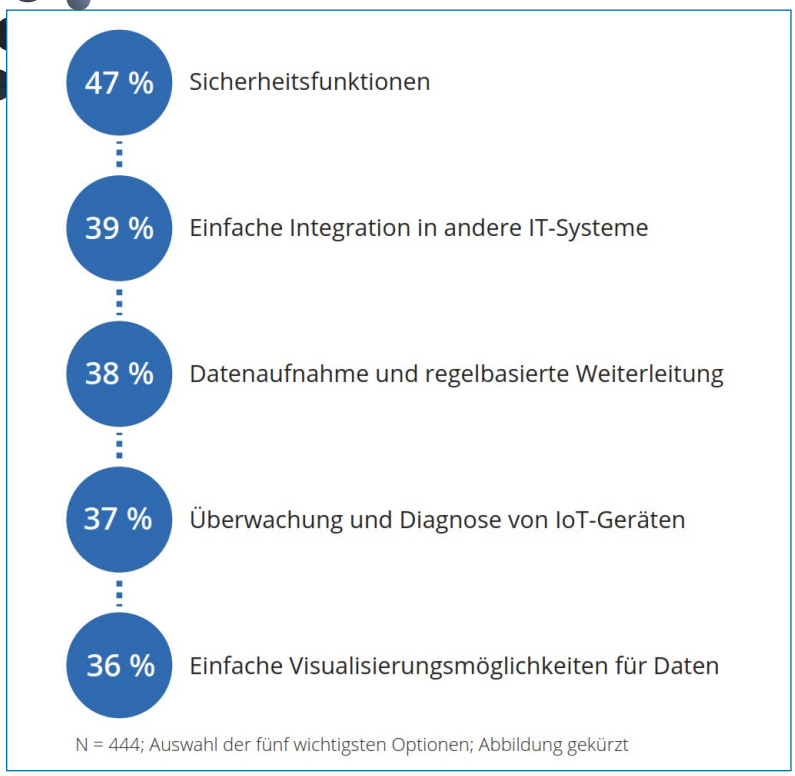
Seitdem hat sich der Begriff vom „Internet der Dinge“ rasant weiter verbreitet und nicht nur Industrieunternehmen, die schon seit viel längerer Zeit ihre Sensoren abgefragt und vernetzt haben (allerdings ohne sich mit den Widrigkeiten des Internets und von TCP/IP herumzuschlagen), sondern auch Hersteller von Consumer-Geräten haben die Vernetzung von Dingen entdeckt: Der vernetzte Kühlschrank, der Toilettenpapier statt Butter bestellt, geistert in diesem Zusammenhang gleichermaßen durchs Feuilleton, die Boulevard-Blätter und die einschlägigen TV-Sendungen.

Der Stand der Dinge: IoT und IIoT im Jahr 2019

Schon im letzten Jahr zeigte es sich auf verschiedenen Messen und Veranstaltungen, wie wichtig die Themenbereiche



rund um IoT und auch um die vielgepriesene Industrie 4.0 für Anbieter und Unternehmen sind beziehungsweise werden. Wer dann in diesem Jahr ganz aktuell einen Blick auf die Hannover Messe Industrie wirft, auf der sich nach dem kläglichen Ende der CeBIT im vorherigen Jahr nun nicht nur die Industriegiganten



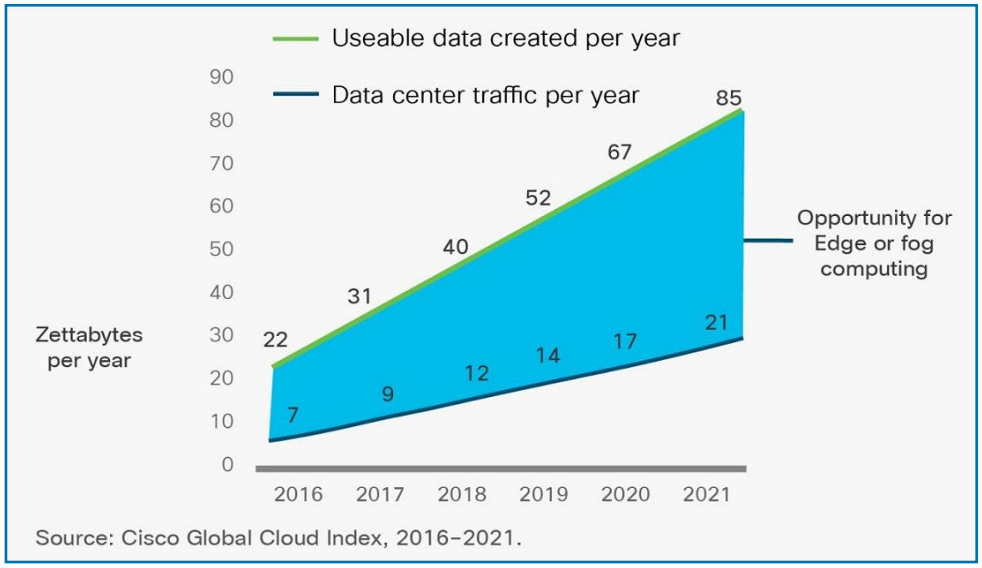
Was erwarten die Unternehmen von IoT-Lösungen? Die Analysten von IDC haben im letzten Jahr bei einer Untersuchung diese fünf Top-Funktionalitäten von IoT-Plattformen ausgemacht. (Bild: IDC Multi-Client-Projekt „Die wichtigsten Technologie-Trends für IoT-Projekte in 2018“)

mit ihren Baumaschinen und Produktionsstraßen, sondern auch alle „Größen“ aus der IT treffen, wird feststellen, dass sich dieser Eindruck im Jahr 2019 weiter verstärkt hat.

Die Analysten von IDC sehen das ganz ähnlich und prognostizierten bereits Anfang dieses Jahres, dass die Ausgaben für IoT mit 745 Milliarden US-Dollar im Vergleich zu 646 Milliarden US-Dollar, die im Jahr 2018 ausgegeben wurden, um 15 Prozent ansteigen werden. Einen jährlich zweistelligen Anstieg dieser Ausgaben bis zum Jahr 2022 sagen sie ebenfalls vorher und gehen davon aus, dass die Ausgaben die Grenze von 1 Billion US-Dollar in jenem Jahr überschreiten werden (Quelle: IDC Worldwide Semiannual Internet of Things Spending Guide). Das zweitgrößte Segment im Umfeld der IoT wird nach Ansicht der Analysten der Consumer-Bereich mit Ausgaben von bis zu 108 Milliarden US-Dollar im Jahr 2019 sein. Dabei stehen die Bereiche Smart Home, Personal Wellness und Connected Vehicle Entertainment an der Spitze dieser Ausgaben. Allein diese Zahlen beweisen, dass IoT schon lange mehr als nur ein Hype-Thema ist. So beobachten viele Experten bereits seit einigen Jahren eine enorme Entwicklung und Verbreitung der „vernetzten Dinge“ in fast allen Bereichen. Eine Aussage der Experten des Unternehmens Fostec & Company, die sich mit Strategieberatung rund um die Schwerpunkte Digitalisierung und E-Commerce befassen, fasst die Situation gut zusammen: „Es ist dabei wichtig zu verstehen, dass es sich beim Internet of Things nicht um eine bestimmte Technologie handelt, sondern vielmehr um ein Zusammenspiel verschiedener Technologien und Anwendungen.“ Ein Eindruck, der gerade durch das breite Angebot an Lösungen für den Bereich Industrie 4.0, wie es in diesem Jahr auf der Hannover Messe Industrie präsentiert wurde, eindrucksvoll bestätigt.

Ein kurzer (konzentrierter) Blick auf die Herausforderungen

Das Internet der Dinge wird von einigen Experten gern auch als „System der Systeme" bezeichnet – eine Ansicht, die gerade aus Sicht der Netzwerk- und IT-Systemprofis durchaus ihre Berechtigung hat. So zeigt eine Betrachtung auf



Wird IoT zum Massenphänomen? Auch die großen Netzwerkausrüster und -anbieter wie Cisco haben daran keinen Zweifel. So warnt Cisco u.a. vor der Flut von Daten (850 ZettaByte; ein ZettaByte entspricht ungefähr 1012 GByte) die bereits 2021 nicht nur von Menschen, sondern auch von Maschinen und „Dingen" erzeugt werden. (Bild: Cisco Global Cloud Index: Forecast and Methodology, 2016–2021)

bestehende IoT- und Industrie-4.0-Projekte, dass sie grundsätzlich aus einer Kombination von Hard- und Software sowie Verbindungstechnik bestehen, die dann in Geschäftsprozesse und den täglichen Betrieb umgesetzt werden müssen. Dabei sehen es beispielsweise die Netzwerkexperten von Cisco in einem Beitrag mit dem Titel „Internet of Things: Challenges, Breakthroughs and Best Practises" als eine sehr wichtige Voraussetzung an, dass sich IT-Fachleute schon bei der Planung von IoT-Projekten mit dem Business-Bereich des Unternehmens absprechen: Diese Menschen verstehen in der Regel sehr viel besser, welche Ergebnisse ein IoT-Projekt aus der Business-Sicht für das Unternehmen bringen soll, während die IT-Abteilung sich eher auf die technische Seite konzentriert. Für diesen Bereich gehen die Cisco-Experten davon aus, dass ein agiles Netzwerk, das auf den neuesten Stand der Technik gebracht wurde, ebenso wie der Zugang zur Cloud und zu Cloud-Speicher essenzielle Voraussetzung für ein derartiges Projekt sein sollten.

Sie weisen aber auch darauf hin, dass der Begriff zwar grundsätzlich alle Projekte umfasst, bei denen es darum geht, „Dinge" mit dem Netz zu verbinden, Daten von ihnen zu bekommen und diese zu analysieren sowie auf die Ergebnisse aus diesen Analysen zu reagieren. Aber sie betonen dabei auch ausdrücklich, dass es für jedes Unternehmen gilt, andere Rahmenbedingungen beziehungsweise einen speziellen Kontext mit in Betracht zu ziehen. Hersteller aus der Industrie wollen und müssen beispielsweise besonderen Wert auf das Monitoring ihrer Produktionsstraßen legen, während es bei Unternehmen aus dem Energiesektor vornehmlich darum geht, Messwerte zu überwachen und beispielsweise frühzeitig auf Abweichungen zu reagieren. So

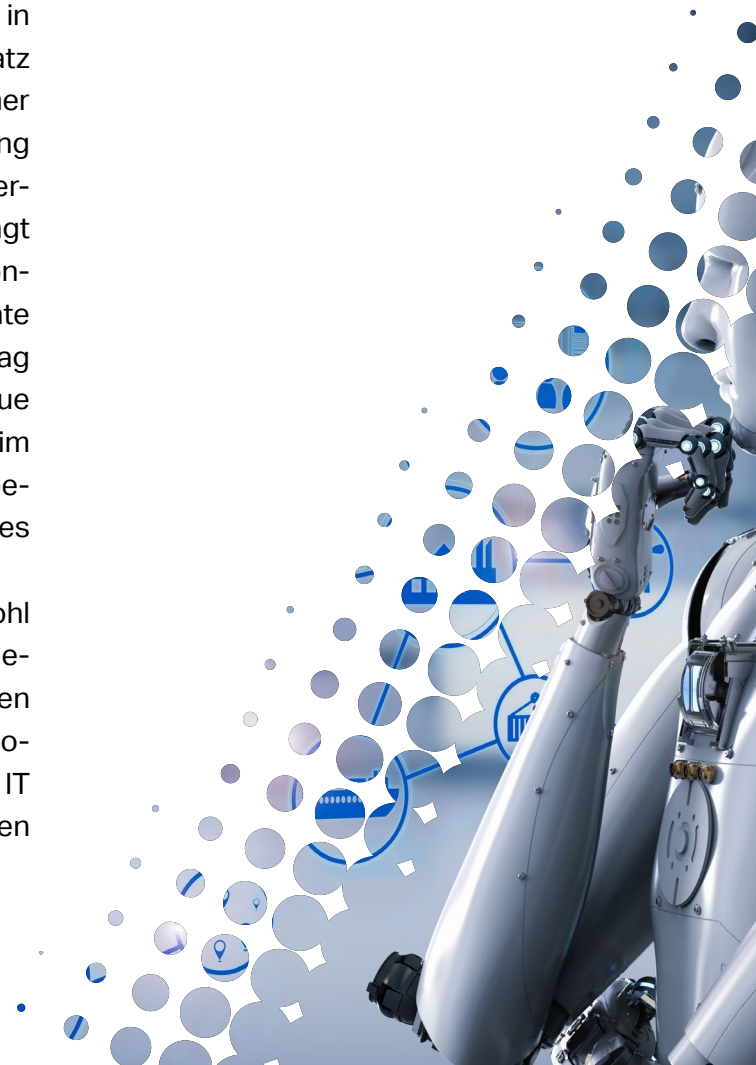
muss dann die IT beispielsweise darauf achten, dass die eingesetzten IoT-Tools problemlos mit anderen Standards und Systemen zusammenarbeiten und Daten austauschen können – ganz gleich ob es um Messgeräte oder die eingesetzten Softwarelösungen geht.

Fazit: Vernetzung ist nicht aufzuhalten – Datenflut muss im Griff behalten werden

Wer mit Profis aus der Industrie redet, wird schnell feststellen, dass die Vernetzung von Sensoren, Aktoren (antriebstechnische Baueinheiten, die vom Steuerungscomputer ausgegebene Befehle in mechanische Bewegungen oder auch in Veränderungen physikalischer Größen wie Druck oder Temperatur umsetzen) und der eigentlichen Produktionsgeräte schon eine ganze Zeit zum Standard gehört. Allerdings kommen in der Industrie beim IIoT und dem Einsatz im Industrie-4.0-Umfeld nun auch immer häufiger die IT-gesteuerte Vernetzung via TCP/IP bis hin zu softwaredefinierten Netzwerken zum Einsatz. Das bringt gerade dort – mehr noch als im Consumer-Bereich – sicherheitsrelevante Probleme (mehr dazu im zweiten Beitrag dieses eBooks) ebenso wie völlig neue Anforderungen bei der Vernetzung im Nahbereich (mit diesen Techniken befassen wir uns im dritten Beitrag dieses eBooks) ins Spiel.

Viele dieser Probleme werden sowohl von den Anbietern als auch von den begeisterten Nutzern solcher Lösungen im Consumer-Bereich einfach ignoriert. Im Bereich der professionellen IT ist es ebenso wie in der traditionellen Industrie nicht möglich, vor solchen Problemen die Augen zu verschließen – allein die wahre Flut an Daten, die solche Techniken zwangsläufig erzeugen, muss sicher beherrscht und kontrolliert werden. Aber nicht nur die gewohnt positiven Prognosen der Analysten und Anbieter solcher Systeme, sondern gerade das Engagement der Industrie machen deutlich, dass diese Entwicklung nicht mehr aufzuhalten ist. Und wenn es nicht unbedingt autonom fliegende Taxis sein müssen, wird die schnelle Verbreitung der IoT-Technik auch im privaten Bereich ihren Weg „zu den Massen" finden.

Thomas Bär und Frank-Michael Schlede



(Un)Sichere Dinge und Probleme

IoT gilt als Triebfeder für die Digitalisierung und die Industrie-4.0-Ambitionen der Menschheit. Leider wurde beim Design nur wenig über die Sicherheit nachgedacht – das könnte sich rächen.

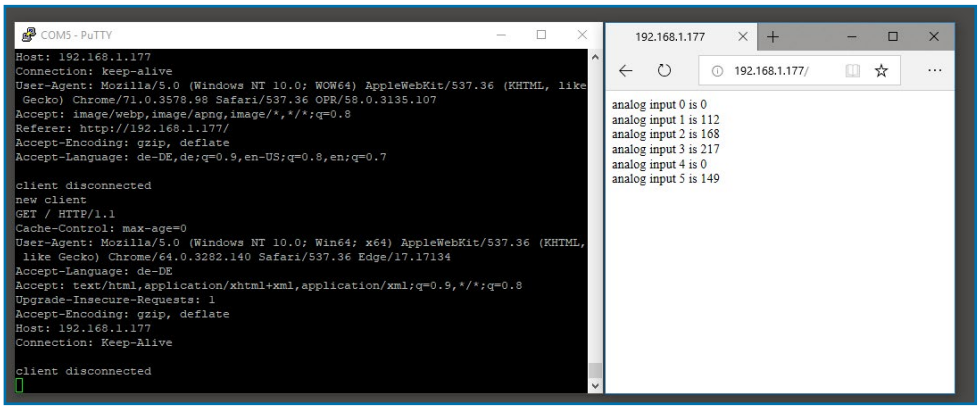
Das Thema IoT wird niemand, sowohl innerhalb als auch außerhalb der IT-Branche, aussitzen können. Die Digitalisierung ist das erklärte Ziel in vielen Unternehmen und was ist in diesem Zusammenhang naheliegender, als langfristig alle Geräte über Internet-Ressourcen ansprechbar zu machen? Denken Sie nur einmal selbst an Ihre Schallplatten/CD-Sammlung zurück – niemand hätte sich 1999 vorstellen können, dass die kleinen mobilen Player einmal auf die komplette Sammlung zugreifen werden können oder dass ein neues Album einfach durch eine monatliche Abgabe hörbar sein wird, oder? Faktisch jedes heute zugelassene Auto könnte über derlei Techniken verfügen, sofern der Kunde es nur wünscht.

An dieser Stelle folgt normalerweise die übliche Auflistung von bereits existierenden oder künftig denkbaren Einsatzgebieten, aber letztendlich ist es unerheblich, ob das Tor der Fertiggarage in absehbarer Zeit über das Smartphone gesteuert schon automatisch öffnet, sobald das Fahrzeug in die Straße einbiegt oder noch immer durch einen kleinen Funkimpulsgeber aktiv geöffnet werden muss. Die Anzahl der Geräte, die mit dem Internet verbunden sind, wächst tagtäglich und gleichzeitig auch die technischen Möglichkeiten.

Unglücklicherweise haben die kleinen Minigeräte, auch wenn sie größte Maschinen in Werkhallen ansteuern, eine Erblast ihrer Vorgänger mit auf den Weg bekommen: Ein grundlegend mangelndes Sicherheitskonzept. Das Internet und ganz besonders dessen Vorläufer, das Arpanet, wurden von ihren Designern als weltweiter Verbund von autonomem Rechnernetzwerken konzipiert, deren Übertragungswege unabhängig von ihrem Inhalt, Absender oder Empfänger durchzuführen sind. Vielleicht ist es ja nur ein moderner Mythos, aber das erste IoT-Gerät der Geschichte soll ein Getränkeautomat an der Carnegie Mellon University in Pittsburgh, Pennsylvania im Jahr 1982 gewesen sein.

Sicherheitstechnisch war für das Internet damals vielleicht noch die Betriebssicherheit beim Ausfall einzelner Knoten bedacht worden, nicht aber die Herausforderung, die sich aus einem grundlegenden Nutzungswandel ergibt. In der frühen Zeit des Internets stellten einige wenige Anbieter Content bereit und die größte Gruppe war damit beschäftigt, auf diese Daten zuzugreifen. Heute generieren User ihren Content selbst und derzeit erleben wir die nächste Entwicklungsstufe, da immer mehr Traffic von den untereinander kommunizierenden IoT-Geräten (M2M) selbst stammt. Das

Internet mutiert zu einem Datensystem der Maschinen – sehr kleinen und sehr großen Maschinen – und es bleibt die Herausforderung des sicheren Betriebs, auch durch den Menschen. Bei einer durch die Analysten von Gartner geschätzten Anzahl von 20 Milliarden Geräten bis 2020 wird rasch klar, dass diese große Gerätezahl eine wahre Herausforderung darstellt.



Kleinsysteme, wie dieser Webserver auf Basis von Arduino, stellen Messdaten einfach und kostengünstig bereit. Problematisch hierbei sind die mangelnde Transparenz bei der verwendeten Firmware und die fehlenden Aktualisierungsmöglichkeiten. (Bild: PuTTY von Simon Tatham, Screenshot: Bär/Schlede)

IIoT: Wo die Sicherheit nicht nur Kühlschrank und Toaster betrifft

Die im vorherigen Absatz genannte Zahl von 20 Milliarden Internet-kommunizierender Devices enthält alle Geräteklassen vom PC und Smartphone über den Fernseher und die Haustechnik bis zur Übertragung von Steuerdaten an Produktionsroboter. Wenn das Internet-Radio aufgrund einer Sicherheitslücke anstelle dem gewünschten Lieblingssender politische Parolen in einer dem Hörer unbekannten Sprache ertönen lässt, ist das in Bezug auf die Eigenschaft irgendwas zwischen unangemessen, ärgerlich oder störend bis nervend. Wenn sich beim Schweißroboter aufgrund einer fehlerhaften Interpretation der Daten die Positionierung um einen Millimeter verschiebt, kann das, je nach Produkt, zu einem Menschenleben gefährdenden Problem werden.

Für eine Unterscheidung des Gerätetyps wurde die Abkürzung „IIoT" auf den Weg gebracht: Industrial Internet of Things. Während bei den herkömmlichen IoT-Devices der Verbraucher oder Anwender im Mittelpunkt des Konzepts steht, sind es hier industrielle Prozesse und Abläufe. Praktischerweise gibt es verschiedene Gruppierungen, die schon jetzt gute Arbeit in Bezug auf Standards und Security-Frameworks auf den Weg bringen. Aber bis ein komplett ausgereiftes System zur Verfügung steht, dauert es nach Expertenmeinung noch. Als Beispiel sei hier das Industrial Internet Consortium genannt, das bereits ein umfassendes Framework für Industrial IoT entwickelt hat und sich aktuell mit detaillierten Dokumenten für den Best-Practice-Einsatz beschäftigt. Ein erstes Dokument, speziell zum Thema Endpoint Security beispielsweise für Sensoren, ist bereits seit 2018 verfügbar.

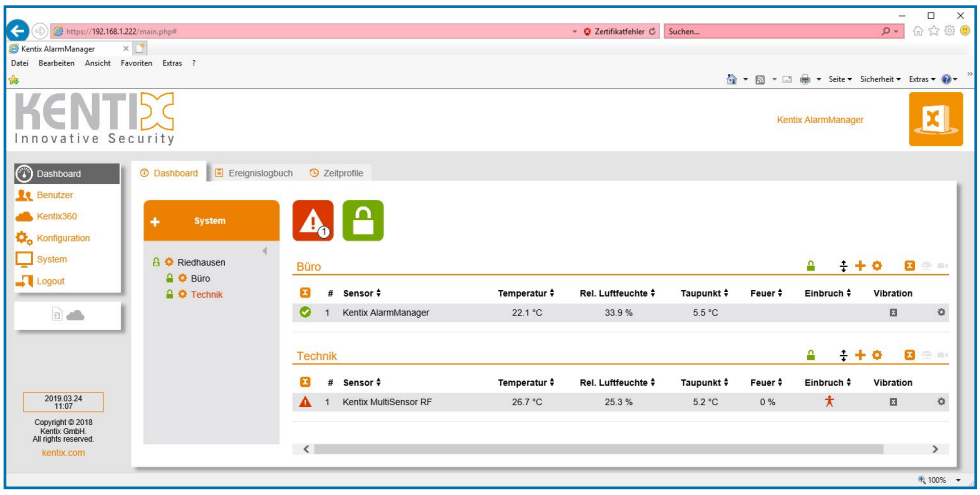
Was können Unternehmen tun, damit IoT nicht zum Security-Desaster wird?

Der bereits abgegriffene Ruf nach einer Sicherheits-Software, früher auch gern Antivirenlösung genannt, kommt auch in diesem Zusammenhang nicht mehr an.

IT-Security hat schon lang nichts mehr mit einfachen „Computerviren“ zu tun. Das Absichern einer Produktionsstraße mit vielen IT-technischen Systemen gelingt nicht durch das Aufspielen einer Software wie auf einen Personal Computer. PCs oder Smartphones sind flexible Hochleistungssysteme für variable Einsatzfelder – ganz im Gegensatz zu Steuerungs- und Messsystemen.

Während die Hersteller dazu übergehen, von Haus aus sicherere Systeme auf den Markt zu bringen, bleiben die Möglichkeiten der Einflussnahme für die Systemadministratoren doch eher beschränkt. Mit einer Ausnahme: dem Gateway. Hier ist jedoch nicht nur der Standard-Router für die Netzwerkverbindung gemeint (wobei ein Teil der Kommunikation sicherlich auch über Netzwerkprotokolle fließt, deren Zusammensetzung sich bei einem Sicherheitsvorfall verändern würde), sondern auch spezielle Geräte. Das IoT-Gateway wandelt die verschiedenen Protokollvarianten, um beispielsweise ältere Systeme mit neuen Strukturen zu verbinden. Bei der Auswahl dieser Systeme empfiehlt sich eine sinnvolle Beschränkung auf die wesentlichen Funktionen, um nicht vollständige OS-Installationen nutzen zu müssen.

Ein überaus kritischer Aspekt im Zusammenhang mit den IoT-Systemen ist die fehlende oder nur schlecht umgesetzte Aktualisierungsmöglichkeit für die Software. Auf der anderen Seite mangelt es oft an einer ausreichend starken Verschlüsselung oder Geräteauthentifizierung. Sofern bei der Anschaffung der entsprechenden IoT-Systeme eine ausreichende Anzahl verschiedener Produktanbieter besteht, ist es eine entscheidende Aufgabe der IT-Verantwortlichen, auf die Aktualisierbarkeit und die Verwaltungsfähigkeiten ein besonderes Augenmerk zu legen. Die Herausforderung hierbei ist die deutlich höhere zu erwartende Einsatzdauer im Vergleich zu klassischen Endbenutzergeräten. Eine Inventarisierung ist logischerweise erforderlich – hier werden die meisten Automatismen für Endpoint-Systeme scheitern, da häufig nicht einmal die einfachsten SNMP-Funktionen in den Kleinstgeräten eingebaut wurden. IT-Leiter sollten sich daher, zumindest in der nächsten Zeit, auf viele manuelle Arbeitsschritte gefasst machen.



Selbst etablierte Überwachungslösungen wie das System von Kentix setzen im Hintergrund auf einfache Datenprotokolle wie ZigBee. Sicherheitstechnisch ist dies, trotz Blockverschlüsselungsalgorithmus AES-128, nicht unumstritten, da alle Geräte dasselbe öffentliche „Fallback Key“-Schlüsselpaar akzeptieren müssen – das ist öffentlich bekannt. (Bild: Kentix StartSet-BASIC, Screenshot: Bär/Schlede)

Letztendlich entscheidet der Kunde über die Ausgestaltung der Sicherheitslösung. Da es um die Verbindung von vollkommen verschiedenartigen Geräten geht, wird der Systemverantwortliche auch mit einer entsprechend hohen Anzahl unterschiedlicher Protokolle und Bussysteme konfrontiert werden. Beim Gebäudemanagement hat sich mit BACnet beispielsweise ein sehr einfaches Verfahren etabliert, das über eine ganz einfache Zweidrahtleitung arbeitet – eine Datenverschlüsselung ist überhaupt nicht vorgesehen. Bei der Auswahl der Gerätetypen gilt es also von Anfang an, mit einem auf die Sicherheit ausgerichteten Konzept zu beginnen und vielleicht bereits begonnene Automatisierungsvorhaben schon jetzt abzubrechen, da sie den Sicherheitsvorstellungen bereits heute nicht mehr entsprechen.

Wer bei der Umsetzung seiner Projekte selbst Hand anlegt und auf einen „technisch ausgeklügelten und sehr leistungsfähigen" 3-Dollar-Chip, wie das ESP8266-WiFi-Modul, und eine im Internet kostenlos angebotene Firmware zurückgreift, muss sich am Ende auch nicht wundern, wenn beispielsweise ein Garagentüröffner auf fremde Kommandos reagiert. Andererseits bieten Plattformen dieser Art dem technisch versierten IT-Profi die Möglichkeit, alle Komponenten selbst zu entwerfen und sich thematisch der Herausforderung zu nähern.

Blockchain und IoT/IIoT

Geht es nach der öffentlichen Wahrnehmung, dürfte Blockchain in erster Linie mit der Finanzbranche in Verbindung gebracht werden. Dabei eignet sich die Technik auch, um die vielen von Sensoren gesammelten Daten sicher zwischen verschiedenen Verarbeitungseinheiten auszutauschen, ohne die komplette Datenmenge stets ins zentrale Rechenzentrum leiten zu müssen. Die Blockchain-Technik speichert Daten automatisch verteilt auf mehrere Rechnersysteme, anstatt sie in einer zentralen Datenbank abzulegen, was die Daten schlussendlich sicherer macht und eine gezielte Manipulation erschwert. Aus der Sicht der IDC-Analysten dürften Blockchain-Mechanismen einen wertvollen Beitrag leisten und ein fester Bestandteil von rund einem Fünftel der IoT-Anwendungsfälle sein.

Aus der Sicht des IT-Entscheiders ist der dynamische und hart umkämpfte IoT-Plattformmarkt derzeit eher unübersichtlich. Den passenden Anbieter und Partner zu finden ist eine Herausforderung. Leistungsstarke Lösungen bieten eine hohe Integrationsfähigkeit von Daten aus unterschiedlichen Quellen. Das Vorhalten flexibler Authentifizierungs-Services im Produkt, Analyse-Fähigkeit, Kapazität „at the edge" und branchenspezifische Referenzen können als Entscheidungshilfe dienen, ob ein Anbieter zum Kunden passt.

Frank-Michael Schlede und Thomas Bär

Wenig Bandbreite, große Reichweite

Im Internet der Dinge müssen eben alle diese „Dinge“ miteinander kommunizieren können – wer schon mal das WLAN in einem großen Hotel am frühen Abend nutzen musste, weiß genau, worauf das hinausläuft. Für IoT müssen andere Techniken her: Ein Überblick über NarrowBand IoT, LoRa und Co.

Mobilfunk-verbindungen (z. B. 3G, LTE, 5G)	Kabelgebundene Verbindungen (z. B. Glasfaser, Kupfer, Powerline)	Nahbereichs-verbindungen (z. B. WLAN, Zigbee, Bluetooth)	Low Power Wide Area Networks (LPWAN) (z. B. LTE-M, NB-IoT, LoRa)	Satelliten-verbindungen (z. B. L-Band, C-Band)
+ Hohe Daten-übertragungsrate + Keine zusätzliche Infrastruktur notwendig	+ Hohe Daten-übertragungsrate + Stabile Verbindung	+ Einfache Anbindung + Vorabbündelung der IoT-Daten im Gateway (Router)	+ Geringer Energie-verbrauch des IoT-Gerätes + Hohe geografische Reichweite	+ Reichweite in abgelegene Gebiete + Reichweite über lange Strecken
– Hoher Batterie-verbrauch des IoT-Gerätes – Keine gleichmäßige Abdeckung	– Positionsverände-rung des IoT-Gerä-tes nicht möglich – Infrastrukturaus-bau schleppend	– Auf kurze Strecken beschränkt – Hoher Energie-verbrauch	– Niedrige Daten-übertragungsrate – Schwer überschau-bares Angebot am Markt	– Hohe Kosten – Nicht geeignet für eine große Anzahl an Verbindungen

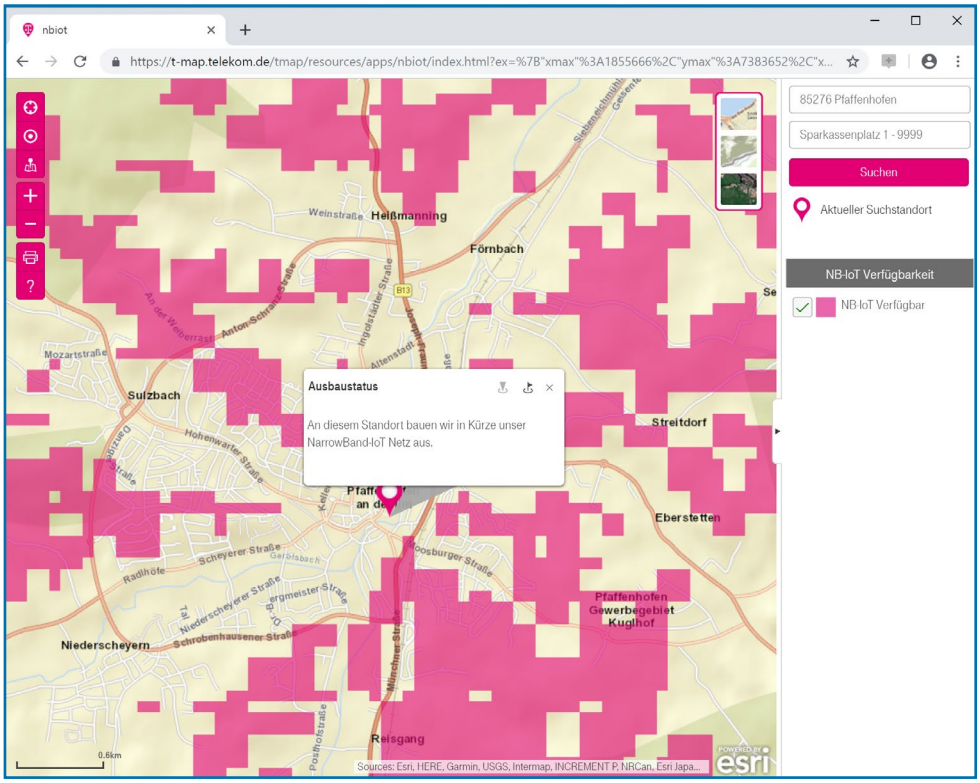
Wie verbinden sich die vielen „Dinge“, die bald im Internet unterwegs sind? Welche Techniken sind für die Kommunikation von „Maschine-zu-Maschine“ (M2M) wirklich geeignet? Die Tabelle zeigt einige Möglichkeiten und auch Grenzen auf. (Bild: IDC Multi-Client-Projekt „Die wichtigsten Technologie-Trends für IoT-Projekte in 2018“)

Mit der Versteigerung der Frequenzen für kommende 5G-Netzwerke kommen die verschiedensten Diskussionen auf: Dabei geht es neben den Themen Kosten, Geschwindigkeit und Abdeckung auch immer wieder um IoT und zwar ganz besonders um die Vernetzung autonomer Fahrzeuge. Viele Experten gehen davon aus, dass diese futuristischen Gefährte ohne ein flächendeckendes 5G-Netz eine der vielen technischen Visionen bleiben werden, die an der praktischen und vor allen Dingen auch sicheren Umsetzung scheitern.

M2M-Kommunikation – Netze wie LTE nicht so gut geeignet

Die-M2M-Kommunikation (Machine to Machine) kann zwar durchaus über vorhandene Netzwerktechniken wie beispielsweise LTE stattfinden, in der Praxis stellt dieses Vorgehen aber sehr häufig nicht die optimale Lösung dar. Sowohl in den Bereichen Abdeckung und Gerätekosten als auch gerade im Bereich Akkulaufzeit, der für IoT-Geräte meist besonders wichtig ist, sind diese bekannten Techniken aus vielerlei Gründen nicht so gut geeignet. Erschwerend kommt hinzu, dass sich die entsprechenden IoT-Geräte nicht unbedingt immer in den idealen Großstadtlagen, sondern häufig auch in Gebieten befinden, die gerade in Deutschland zu den vielen weißen Flecken bei der Abdeckung durch die Mobilfunk-Netze

gehören. Auch die Tatsache, dass solche Geräte, die in GSM-, 3G- oder LTE-Netzwerken arbeiten, für viele Dienste (wie Sprache, Nachrichtenübertragung und schnelle Datenübertragung) konzipiert sind, macht sie für die Einsatz in IoT-Geräten wenig brauchbar.



Wer wissen will, ob seine IoT-Geräte schon die richtige Technik im „heimatlichen Umfeld" finden, kann auf der Webseite der Telekom nachprüfen, ob NarrowBand IoT auch an seinem Standort verfügbar ist. (Bild: Telekom)

Hier sind kleine, wenig komplexe Geräte gefordert, die einen geringen Stromverbrauch und eine entsprechende Funkverbindung aufweisen. Hier kommen dann zur Vernetzung Konzepte wie LPWAN (Low Power Wide Area Network) oder LPN (Low Power Network) zum Einsatz, denen eine hohe Netzabdeckung in Kombination mit einem geringen Energieverbrauch gemein ist.

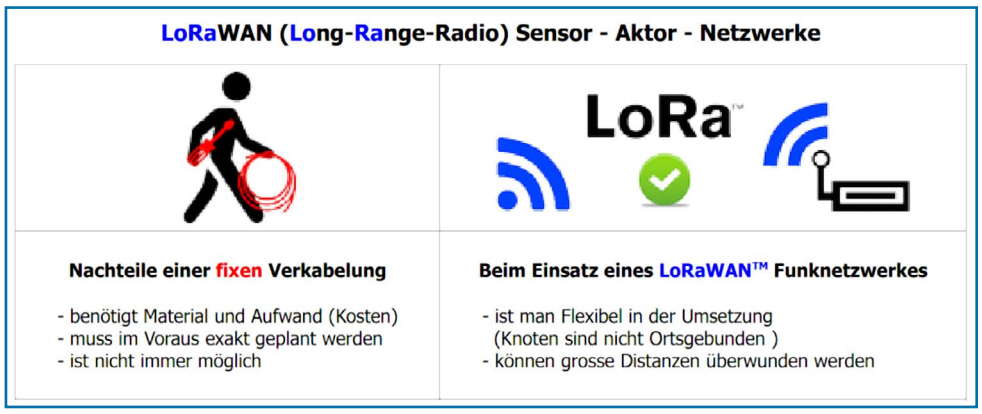
LPWAN und die Standards

LPWAN wird zwar mit großer Wahrscheinlichkeit in jeder Diskussion, die sich um die IoT-Geräte und deren Vernetzung dreht, ein Thema sein, aber es ist dabei wichtig hervorzuheben, dass LPWAN an sich keinesfalls ein Standard ist. Es ist die weitgefasste Bezeichnung für verschiedene Implementierungen und auch Protokolle aus diesem Umfeld. Dazu zählen dann sowohl proprietäre als auch verschiedene Open-Source-Ansätze. Bei all diesen Netzen geht es um eine möglichst hohe Abdeckung gepaart mit geringem Energieverbrauch. Dabei werden in der Regel keine großen Nachrichten hin- und hergeschickt, oftmals sind es nur wenige Kilobyte, die ihren Weg über die Funkstrecke finden. Die Anwendungen, die darauf aufsetzen, müssen deshalb auch dazu in der Lage sein, mit geringer Bandbreite und großer Latenz zurechtzukommen.

3rd Generation Partnership Project (3GPP) ist ein Zusammenschluss von verschiedenen Gremien, die unter anderem für die Standardisierungen im Bereich des Mobilfunks verantwortlich zeichnen. Im Jahr 2016 wurde eine Reihe von Technologien, die speziell für den

IoT-Einsatz optimiert wurden, von 3GPP entwickelt, die auch unter der Bezeichnung „Mobile IoT" bekannt wurden. Dazu gehören unter anderem die Techniken NarrowBand IoT (NB-IoT) und LTE-M (Long Term Evolution for Machines), zwei Bereiche, in denen sich die Telekom besonders stark engagiert.

NB-IoT verwendet dabei als Grundlage die bestehende LTE-Technik. Das bedeutet, dass auch Ressourcen wie Antennen, die Basisstationen, Standorte der LTE-Netzbetreiber und so weiter von dieser Technik benutzt werden. Obwohl LTE hier als Grundlage fungiert, wurden Besonderheiten der jeweiligen Spezifikation, die für LPWA nicht notwendig sind, hier bewusst ausgespart. So ist NB-IoT in der Lage, kleine Datenmengen in großen Zeitabständen auch unter schwierigen Bedingungen und über große Distanzen zuverlässig zu übertragen. Durch die Einschränkungen sowohl bei der Sendefrequenz als auch bei der verwendeten Datenrate sind Endgeräte möglich, die einen erheblich geringeren Strombedarf haben und so auch jahrelang mit nur einem Batteriesatz funktionieren können. Mit anderen LPWA-Techniken eint NB-IoT, dass es grundsätzlich einen besseren Empfang in Gebäuden ermöglicht. Die Techniker sprechen hier von einer guten „Festkörperdurchdringung", die es ermöglicht, diese Geräte dann teilweise sogar in den Untergeschossen von Gebäuden problemlos zu betreiben.

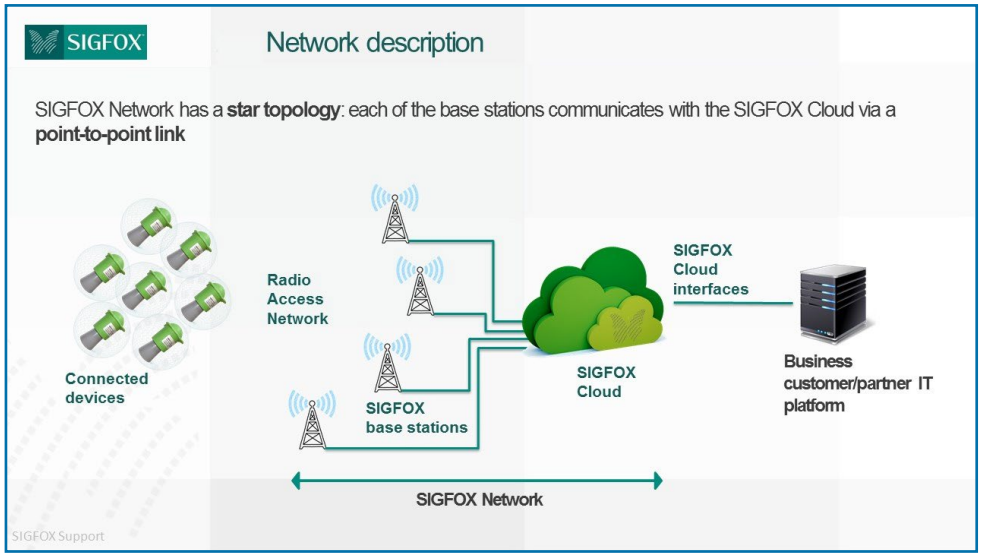


Verkabeln oder Geräte über LoRaWAN ins Netz bringen? Diese Gegenüberstellung zeigt sehr deutlich, was mehr Vorteile im praktischen Einsatz bringt. (Bild: Iset)

Weitere Übertragungstechnologien: LoRa (LoRaWAN) und Sigfox

Während die NB-IoT-Technik im lizenzierten Spektrum angesiedelt ist, verwenden die Techniken LoRa/LoRaWAN und Sigfox das nicht lizenzierte Spektrum für die Übertragung. National ist im lizenzierten Spektrum die Bundesnetzagentur für Zuweisung und Registrierung der Sende- und Empfangsfrequenzen zuständig. Das unlizenzierte Spektrum, in dem sich LoRa und Sigfox bewegen, ist im Prinzip frei nutzbar, solange gewisse Mindeststandards eingehalten werden. Alle drei Techniken bieten bidirektionale Datenübertragung im Halbduplex-Verfahren. LoRa und Sigfox zielen dabei auf einen ganz bestimmten Bereich des IoT-Marktes ab: Sie kommen bereits bei vielen einfachen Geräten zum Einsatz, bei

denen es vor allen Dingen auf sehr lange Lebensdauer der Batterien bei gleichzeitig begrenzter Bandbreite ankommt.
Die Lora-Alliance ist eine offene Non-Profit-Organisation, zu der nach eigenen Aussagen aktuell mehr als 500 Firmen (unter anderem auch IBM und Cisco) zählen. Sie haben es sich zum Ziel gesetzt, LPWAN-Techniken im großen Stil zu verbreiten. LoRaWAN wird dabei



Das Sigfox-Netz im Überblick: Es verwendet eine Stern-Topologie, die direkt mit der SigFox-eigenen Cloud-Lösung verbunden ist. Es eignet sich besonders gut für Anwendungen, bei denen die Systeme nur unregelmäßig kleine Datenmengen senden müssen. (Bild: Sigfox)

von dieser Allianz als „Open-Standard Network Layer" bezeichnet. Während LoRa die rein physikalische Schicht (also den eigentlichen Chip) darstellt, ist LoRaWAN der MAC-Layer (Media Access Control) – also die Software, mit deren Hilfe die gemeinsame physische Verbindung der Systeme mit dem Netzwerk überhaupt erst möglich ist. LoRaWAN definiert somit sowohl das Kommunikationsprotokoll als auch die Systemarchitektur für das Netzwerk.

LoraWAN bietet eine ganze Reihe von Vorteilen: So kann ein solches Netz sowohl im Innenbereich Sensoren und Aktoren relativ problemlos über viele Stockwerke hinweg einbinden. Im Freien kann die Technik diese Geräte bei Sichtkontakt sogar bei Distanzen einbinden, die größer als 10 Kilometer sind. Dabei liegen die Sendeleistungen deutlich unter denjenigen eines WiFi-Netzwerks. Die Datenübertragung ist verschlüsselt und besitzt laut Aussagen von Experten eine hohe Resistenz gegenüber Störeinflüssen. So bietet die Technik im Prinzip die Reichweite eines Mobiltelefons gekoppelt mit einer Flexibilität, wie sie Anwender von Bluetooth- oder Wifi-Verbindungen her kennen, bei einem Energieverbrauch, der eher dem einer Armbanduhr (keiner Smartwatch!) ähnelt. Allerdings ist das alles nur mit einer sehr geringen Datenrate möglich. LoraWAN eignet sich deshalb ideal für Gerät, die nur wenige Daten in unregelmäßigen Abständen senden müssen. Beispiele sind Anwendungen für Parkplatzsuche und -zuweisung (Smart Parking) oder auch die Kontrolle von Straßenbeleuchtungen.
Neben anderen Techniken hat auch Sigfox bereits genügend Verbreitung gefunden. Die französische Firma gleichen Namens hat ihre proprietäre Technik besonders im europäischen Raum etablieren können. Das Unternehmen hat ein eignes Funknetz (Sigfox-Netz)

zusammen mit Servern in der Cloud aufgebaut und strebt nach eigenen Angaben eine EU-weite Abdeckung an. Das Protokoll nutzt dabei die sogenannte Ultra-Narrow-Band-Technik (UNB). Sie ermöglicht es, sehr viele Objekte mit geringem Datenaufkommen und Energiebedarf drahtlos mit dem IoT-Netz zu verbinden.

Deshalb eignet sich diese Technik auch besonders gut für Anwendungen, bei denen das System beziehungsweise die Sensoren und Aktoren nur kleine Datenpakete in unregelmäßigen Zeitabständen senden müssen.

Der entscheidende Unterschied zu den zuvor geschilderten Ansätzen besteht darin, dass dieses Protokoll, das dahinterstehende Netz sowie die Infrastruktur der verwendeten Cloud und die Technik proprietär sind. Unternehmen, die ihre IoT-Geräte mit Sigfox anbinden und betreiben, sind daher auf diese Firma angewiesen.

Thomas Bär und Frank-Michael Schlede

Riesige Datenmengen und Roboter

Die Zukunft beginnt schon jetzt – durch die zunehmende Verbindung von Robotern, Sensoren und Automatisierungslösungen entsteht der volldigitale Lebenszyklus von Produkten.

Gern benutzen Anbieter wie auch Industrieunternehmen die Bezeichnung „Industrie 4.0", wenn es um die Digitalisierung geht. Kaum verwunderlich, handelt es sich doch bei dem Zukunftsprojekt um eine komplette und allumfassende Digitalisierung der industriellen Produktion. Historisch wird die erste industrielle Revolution mit der Mechanisierung mittels Wasser- oder Dampfkraft in Verbindung gebracht. Fließbänder und Massenproduktion kennzeichnen die zweite industrielle Revolution. Der Einsatz von IT und Elektronik wird als die dritte Revolution bezeichnet und der nächste Schritt soll durch intelligente und digital vernetzte Systeme gekennzeichnet sein, so Wikipedia.

Industrie 4.0 ist jedoch nicht nur eine Zukunftsvision. Schon jetzt gibt es auch mittelständische Unternehmen, die ihre Produktion auf „Smart Factory" umstellen. Das im mittelhessischen Haiger ansässige Familienunternehmen Rittal, bekannt für IT-Schranksysteme, verkündete beispielsweise vor Kurzem, dass die Kompaktschrankproduktion komplett auf Industrie-4.0-Kriterien umgestellt wird. Insgesamt investiert der Hersteller 250 Millionen Euro. In den neuen Fabrikhallen, so der Hersteller, werden bald mit mehr als 100 neuen Hightech-Maschinen und Anlagenkomponenten auf 24.000 Quadratmetern hochautomatisiert rund 9.000 AX-Kompaktschalschränke und KX-Kleingehäuse pro Tag gefertigt. Dafür wird das Werk rund 35.000 Tonnen Stahl pro Jahr verarbeiten.

Selbst in der deutschen Großindustrie ist der IoT/Cloud-Gedanke nunmehr angelangt und dies auch in der Autoindustrie – beim Volkswagen Konzern. Der Wolfsburger Autokonzern und Amazons Cloud-Sparte AWS sind eine enge strategische Partnerschaft eingegangen. In der „Volkswagen Industrial Cloud" gilt es, die Echtzeitdaten von 122 Werken darzustellen. Das erklärte Ziel hierbei: Die Daten aus den Werksbereichen zu sammeln, zu analysieren und die Erkenntnisse über die Fertigung als Grundlage für eine Optimierung der Produktion und Verbesserung der Prozesseffizienz zu nutzen.

Andere Spielregeln

Für die Industrie gelten, nicht nur bei IIoT/IoT, andere Regeln als für den gewöhnlichen Einsatzfall. IIoT-Systeme unterscheiden sich deutlich im Bereich der Komplexität. In einem Smart Home steuert der Besitzer über sein Smartphone einige wenige Parameter wie die Heizung oder die Rollläden. In einer „Smart Factory" arbeiten hunderte,

wenn nicht gleich tausende hochpräzise Sensoren und messen kontinuierlich eine riesige Masse an Werten. Ähnlich verhält es sich bei der GPS-Positionierung. Das Auffinden des eigenen Fahrrads per App unterscheidet sich doch deutlich von der Überwachung der Kühlketten von Hochseecontainern.

Aktuell investieren viele Firmen in Robotertechnik und Smart-Factory-Vorhaben. (Bild: Rittal)

Roboterzukunft ohne IoT denkbar?

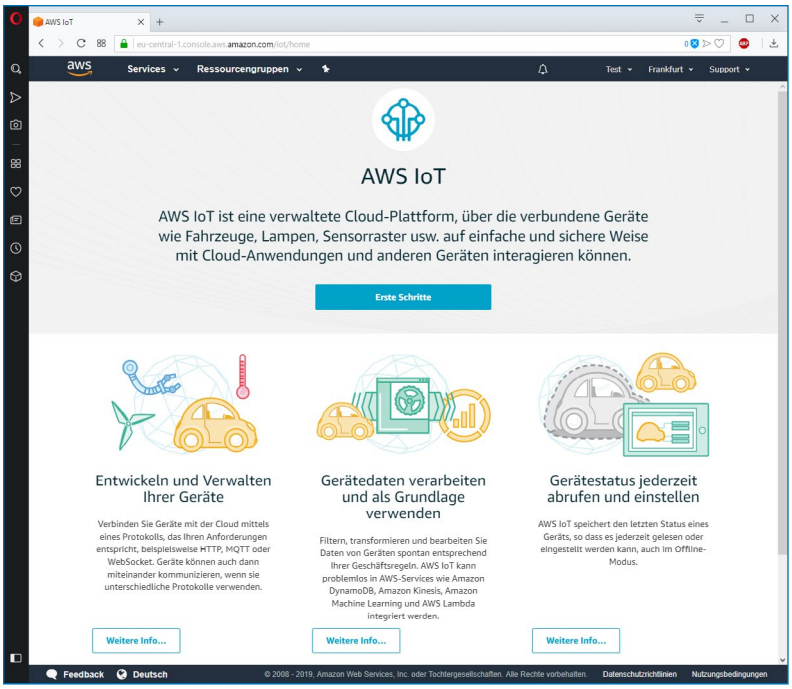
Es ist wohl verfrüht, zu behaupten, dass in kürzester Zeit alle Produktionssysteme, Maschinen und Roboter zwangsläufig als IoT-Devices zu betrachten wären. Wer die Lebensdauer dieser Systeme kennt, weiß, dass es hier Produktzyklen von Jahrzehnten geben kann. Alle jüngeren Systeme verfügen selbstverständlich über Netzwerksteuerungen und in absehbarer Zeit dürften die meisten Systeme auch untereinander direkt vernetzbar sein.

Vollautomatische Kommissioniersysteme, beispielsweise im Arzneimittelgroßhandel, wurden zunächst von einem zentralen Computer gesteuert. Um die Echtheit eines Medikaments zu prüfen, übermittelt schon heute ein vorgelagerter oder integrierter Scanner die individuellen, serialisierten Chargendaten an eine über das Internet ansprechbare „securPharm"-Datenbank. Je nach Konzept arbeiten verschiedene, an sich getrennte Systeme gemeinschaftlich am Vorgang der Prüfung, Sortierung, Erfassung und Bereitstellung zusammen.

Es ist nur naheliegend, mittel- bis langfristig alle Systeme mit Kommunikationstechniken auszustatten, um sie so zu einem IoT-Device werden zu lassen. Wenn ein herkömmlicher Tintenstrahldrucker automatisch eine Nachbestellung von Tinte einleiten kann, warum soll ein Notstromdiesel nicht ebenfalls seine Flüssigkeitsstände per Sensor überwachen und Wartungszeiten per Automatismus einfordern? Selbiges gilt für Flüssiggaslagerstätten, Heizungssysteme, e-Roller oder Sortiermaschinen – die Liste lässt sich beliebig verlängern.

Sicherlich wird es auch hier Grenzen geben. Den automatischen Interaktionen von Systemen im Gesundheitswesen hat der deutsche Gesetzgeber im Medizinproduktgesetz (MPG) beispielsweise klare Grenzen auferlegt. Es gibt, je nach

Branche, verschiedene Einschränkungen, die den Einsatz von IoT-Systemen in der Praxis limitieren könnten. Oft folgt ein rechtlicher Rahmen erst mit einigen Jahren Verspätung und ermöglicht so erst verzögert die Verwendung moderner Techniken.



Amazons AWS ist nur eine der vielen verwalteten Cloud-Plattformen für IoT-Systeme. (Bild: Amazon)

Riesige Datenmengen und totale Vernetzung

Die Datenmenge im Internet und den lokalen Netzwerken wächst unaufhörlich. Sofern die Berechnung des Internet-Dienstleisters Robert Löffler stimmt, wächst das Internet um 70 Terabyte pro Sekunde, sodass es bei dieser Artikelerstellung schon einen Umfang von 14.855.088 Petabyte an Daten fasste. Während sich das durchschnittliche Datenvolumen eines privaten Breitbandanschlusses von 44,2 GByte pro Monat im Jahr 2018 laut Statista verdoppelt hat, können insbesondere Netzwerkadministratoren den IoT/IIoT-Entwicklungen ein wenig gelassener entgegensehen.

Systembedingt ist ein großer Teil des Internets verborgen, ohne näher auf die Besonderheit des „Dark Webs“ oder der „Private Public Cloud“ eingehen zu wollen. Viele gesammelte Daten sind schlichtweg Server-Log-Files oder andere Protokolldaten, die eher lokal zur Speicherung anfallen. Es ist zudem überhaupt nicht erforderlich, alle Sensordaten direkt vom IoT-Device in das Rechenzentrum zu transportieren. IoT-Systeme sollen über das „Edge Computing“ die Datenmenge kleinhalten. Dahinter steckt die Idee, dass vor allem die bei der Verarbeitung oder Vorverarbeitung erfassten Daten direkt bei ihrer Entstehung im Gerät oder in einem Steuersystem in unmittelbarer physischer Nähe verarbeitet werden. Mitunter könnte das System so sogar eine gewisse Zeit lang auf eine ständige Internetverbindung verzichten.

Klassischerweise sollen Router als IIoT-Gateways fungieren und so ein intelligentes und steuerbares Bindeglied zwischen dem Cloud-Dienst und der lokalen Anwendung, der „Edge“, bilden. Router können die entstehende Datenmenge vor der Übertragung auf die wesentlichen Informationen verdichten und so Zeit und auch Kosten sparen.

Das Szenario der „totalen weltweiten Vernetzung“ geistert so manchem Marktbeobachter irgendwann zwangsläufig durch den Kopf. Wer die Entwicklung der letzten Jahre betrachtet, wird ohne Zweifel erkennen, dass dieser Vorgang in der Tat voranschreitet. Vor zehn

Jahren war ein Fernseher noch ein Standalone-System, heute ist eine Internetanbindung selbstverständlich, ebenso die Unterstützung für Mira oder Apple-Cast, der eingebaute Bluetooth-Adapter oder die WiFi-Einbindung. Was für Fitnesstracker, Smartwatches, Smartphones, Tablets und Autos gilt, ist auch auf Maschinen und Produktionsanlagen anwendbar.

Cloud kann und muss helfen

Scheinbar sind Cloud Computing und IoT technologisch fest miteinander verbunden. Es wäre zwar möglich, Funktionalitäten losgelöst von Cloud-Techniken abzubilden, jedoch ist es in der Regel wenig zielführend. Die „IoT-Cloud" entsteht zwangsläufig aus dem Wunsch der Datenminimierung, so die Experten von IDC. Die Analysten gehen davon aus, dass schon heute rund 40 Prozent der IoT-Daten „at the edge", also im oder in der Nähe des vernetzten Objekts, verarbeitet und analysiert werden.

Die „Wolkenbildung" entsteht folglich von allein. Firmen werden auch weiterhin vor diesem Hintergrund von Hardware-Herstellern eine offene IoT-Gateway-Lösung, von Communications Service Providern Network-Function-Virtualization-Fähigkeiten (NFV) und von Analytics-Anbietern Funktionen „at the edge" einfordern.

Cloud Computing ist somit so etwas wie die Haupttriebfeder für IoT. Wie schon das Grid Computing senkt auch das Cloud Computing die Kosten, indem es die vorhandenen Ressourcen maximal ausnutzt. Eine IoT-Cloud ist eine Art fertiger Technologie-Stack, der dabei unterstützt, Dinge mit Backend-Komponenten oder aber auch mit anderen IoT-Devices kommunizieren zu lassen. Im Idealfall sind alle Technologien wie Integration, Schnittstellen, Big Data, Geräteverwaltung und Analysefunktionen in diesem Stack einheitlich zusammengefasst. Es besteht zwar generell die Möglichkeit, die einzelnen Bestandteile selbst miteinander zu kombinieren, jedoch setzt dies ein extrem gutes Know-how der Techniken voraus. Die Mehrheit der Interessenten wird sich für ein oder mehrere fertig konfektionierte Angebote entscheiden (müssen). Namhafte Anbieter sind Amazon Web Services (AWS), Windows Azure von Microsoft, die Oracle Cloud oder das Angebot von Q-Loud.

Mag sein, dass es sich bei Industrie 4.0 ein wenig mehr um ein Buzzword handelt, da der eklatante Unterschied zum vorherigen Entwicklungsschritt auf den ersten Blick nicht ganz so groß wirkt. Wie man sich selbst hier positioniert, ist auch nicht wirklich entscheidend, denn die Entwicklung IoT und Industrie 4.0 ist bereits weit fortgeschritten und beginnt nun die Produktionswelt zu verändern. Sollte der Ausbau der 5G-Netze tatsächlich schnell vorankommen, verlieren lokalisierte Netzwerkstrukturen zunehmend ihre Notwendigkeit. Und schon scheint eine Ansteuerung von Produktionsanlagen aus dem Cloud-Service realistischer. Letztendlich sind Bits viel einfacher zu bewegen als Atome.

Frank-Michael Schlede und Thomas Bär