Revolution im Alltagsleben

Mit der Pandemie und dem damit verbundenen Anstieg an Fernarbeitsplätzen hat das Internet der Dinge (IoT) noch einmal einen zusätzlichen Schub erhalten. Die Menschen sind schon online, jetzt werden immer mehr Dinge vernetzt. *Von Dirk Mewis*

Statistisch gesehen, platzt in Deutschland alle 30 Sekunden ein Wasserrohr und verursacht Schäden in Höhe von mehr als drei Milliarden Euro pro Jahr. Gemeinsam mit Eon stattet Vodafone inzwischen Wasserzähler mit einer intelligenten Funktechnologie aus, die in der Lage ist, Unregelmäßigkeiten im Wasserverbrauch zu erkennen, vor geplatzten Wasserrohren zu warnen und Ressourcen einzusparen.

Denn längst sind nicht mehr nur Smartphones über Mobilfunk vernetzt. Auch Maschinen, Roboter und zahlreiche Alltagsgegenstände kommunizieren im Netz: Autos, Fahrräder, Spielzeuge, Schiffscontainer, Umweltsensoren, Mülleimer oder Parkplätze. Ein Ding im Internet der Dinge kann beispielsweise ein Arbeitshelm für Bauarbeiter sein, der einen Notruf absetzt, sobald er ungewöhnlich starke Stöße oder Stürze bemerkt, oder eine Milchkanne, die sich meldet, sobald sie wieder aufgefüllt werden muss.

Beschleuniger 5-G-Mobilfunk-Netz

Das Internet der Dinge ist mittlerweile aus dem Alltag vieler Menschen nicht mehr wegzudenken. Dabei wissen wir in vielen Fällen gar nicht, dass die Gegenstände und Services, die wir nutzen, so nur funktionieren, weil sie längst im Internet der Dinge funken. Die Ausbreitung wird jetzt durch den Fortschritt beim Ausbau des 5-G-Mobilfunk-Netzes noch mal beschleunigt, denn der neue Mobilfunk-Standard kann noch mehr Gegenstände zeitgleich vernetzen als bisherige Mobilfunk-Technologien. Mehr als 160 Millionen Gegenstände funken weltweit im Vodafone-Netz. Tendenz: rasant steigend.

In nur zwei Jahren hat sich die Zahl der vernetzten Gegenstände um mehr als 50 Prozent erhöht. Die Vernetzung von Alltagsgegenständen oder Maschinen über das Internet funktioniert in vielen Fällen über Mobilfunk. Ausgestattet mit Sensoren, kleinen Chips und SIM-Karten, können Gegenstände erfasste Daten (wie zum Beispiel Bewegungsdaten oder Temperaturdaten) via Mobilfunk übermitteln, um so eine Reaktion auszulösen – automatisch oder wiederum individuell ausgelöst durch Menschen. Daher werden die vernetzten Gegenstände auch häufig als smart oder intelligent bezeichnet.

Die Deutsche Telekom vernetzt die Herzschrittmacher des Berliner Medizintechnikspezialisten Biotronik und übermittelt die Gesundheitsdaten der Patienten an den behandelnden Arzt. Der Arzt bekommt automatisch täglich Informationen über den Zustand des Herzschrittmachers sowie über den Patienten und kann bei einer Verschlechterung schnell eingreifen. Schlägt das Herz langsamer oder unregelmäßig? Besteht die Gefahr von Vorhofflimmern?

„Je früher der Arzt Informationen erhält, desto früher kann eine medikamentöse Therapie begonnen und können kritische medizinische Situationen vermieden werden. Das Versenden der Daten funktioniert nicht nur innerhalb Deutschlands, sondern sogar weltweit zum behandelnden Arzt“, erklärt Volker Lang, Senior Vice President Research & Development bei Biotronik.

Klinische Studien belegen inzwischen, dass die Sterblichkeitsrate bei Patienten mit einem vernetzten Herzschrittmacher um 60 Prozent reduziert werden konnte. Außerdem zeigte sich, dass beim Einsatz des vernetzten Herzschrittmachers, im Vergleich zur klassischen Behandlung, auf 81 Prozent der üblichen ambulanten Präsenztermine zur Nachsorge verzichtet werden konnte.

Die Ausgaben für IoT-Anwendungen sind nach Angaben von Statista von 2016 bis 2020 von 1,35 auf 2,95 Billionen US-Dollar gestiegen. Die Wachstumsrate übertrifft mit über 25 Prozent pro Jahr den Zuwachs in der gesamten IT-Branche deutlich. Und schon bald, so die Erwartungen der Marktforscher, dürften zehnmal mehr Dinge auf der Welt vernetzt sein als Menschen.

IoT im Liefer- und Versandhandel: Bewegungsaktivierte Smart-Kameras, intelligente Regale und RFID-Technologien helfen dabei, Artikel zu finden, und erleichtern den Austausch von Bestandsinformationen.

FOTO WAVEBREAKMEDIAMICRO/ADOBE STOCK

Das intelligente, oft KI-gestützte Zusammenspiel aus vernetzten Komponenten wie Mikrocontrollern, Sensoren sowie Aktoren, die elektrische Impulse in Druck, Bewegung, Temperatur oder andere mechanische Größen umwandeln, ermöglicht das Internet der Dinge. Die IoT-Systeme verknüpfen einzelne Geräte, Datenbanken und sogenannte Gateways. Über eine meist drahtlose Schnittstelle sind sie ans Internet angebunden und versenden Daten oder erhalten umgekehrt Befehle. Im Hintergrund werden die sensiblen Informationen bei der Übertragung durch Sicherheitslösungen geschützt und gesichert.

Immer mehr Unternehmen betrachten IoT als wichtiges Element für den Geschäftserfolg. Laut einer Studie von Microsoft im Jahr 2020 unter 3000 Entscheidungsträgern, die an IoT-Entscheidungen in Unternehmen beteiligt waren, betrachteten 90 Prozent der Unternehmen das Internet der Dinge als entscheidend für den Gesamterfolg ihres Unternehmens.

KI-gestützte Vernetzung

So nutzt die Einzelhandelsbranche beispielsweise Cloud-KI in IoT-basierten Diensten, um ihre Kundenerlebnisprogramme zu erweitern und Produkte zu verbessern. Oder Reeder, Versender und Cloud-Anbieter übernehmen reihenweise Spezialfirmen für Datenanalyse. Die massiven Störungen im Schiffs- und Bahnverkehr, seit Monaten verantwortlich für Produktionsengpässe und leere Regale im Handel, befeuern in der Logistik das M&A-Geschäft. Bevorzugtes Ziel sind Software-Dienstleister, die anhand von Datenbanken, Künstlicher Intelligenz und Tracking-Lösungen treffsicher voraussagen können, wann die Importwaren die Kundschaft erreichen, um so durch gezielte Auswertung die Lieferengpässe zu überwinden.

Auch der Logistikriese DHL ist von der wachsenden Bedeutung der Künstlichen Intelligenz überzeugt. Sie werde benötigt, um Veränderungen in der Verbrauchernachfrage zu antizipieren, was sich auf die Bestands- und Transportpolitik der Einzelhändler auswirke. Darüber hinaus könne KI bei der Gestaltung von Lieferketten entsprechend der Nachfrageentwicklung und der Lagerwirtschaft hilfreich sein. Die Logistikprofis prognostizieren daher, dass sich der weltweite Markt für Roboter und Lagerautomatik bis 2025 auf rund 27 Milliarden US-Dollar verdoppeln werde.

Sicher in der Datenwolke

Cloud-Technologie gilt als Hebel für die digitale Transformation in Unternehmen. Die große Mehrheit der Unternehmen setzt dabei auf Hybrid- und Multi-Cloud-Systeme.

Von Harald Czycholl

Vernetztes Auto: Ein gutes Navigationssystem ist vor allem im E-Auto Gold wert.

FOTO WILLIAM/ADOBE STOCK

Einen Parkplatz suchen, eine E-Ladesäule finden, einen Stau umfahren: All das ist bereits im Auto realisierbar. Über Clouds stellen die Autohersteller ihren Kunden zahlreiche Services zur Verfügung, die diese in ihren jeweiligen Fahrzeugen direkt nutzen können – moderne Autos werden mehr und mehr zu rollenden Computern. Auf der anderen Seite nutzen die Fahrzeughersteller die Vorteile der Cloud selbst auf vielfältige Weise, um ihre Betriebskosten zu dämpfen und ihre Partner besser anzubinden.

Der Volkswagen-Konzern zum Beispiel hat mit der Volkswagen Automotive Cloud und der Volkswagen Industrial Cloud zwei große Cloud-Systeme, die sehr unterschiedliche Dinge machen. Während über die Volkswagen Automotive Cloud die verschiedenen Features für die Fahrer gesteuert werden, sorgt die Volkswagen Industrial Cloud für eine Vernetzung der 124 VW-Werksstandorte – und soll im nächsten Schritt auch die rund 1500 Zulieferer integrieren. Und die beiden VW-Clouds verfolgen nicht nur unterschiedliche Zwecke, sondern werden auch von verschiedenen Anbietern bereitgestellt: Für die Industrial Cloud greift Volkswagen auf die Dienste von Amazon Web Services (AWS) zurück – und für die Automotive Cloud auf Microsofts Azure-Cloud.

Private Cloud oder Public Cloud

Geschwindigkeit, Kostenvorteile, Zukunftssicherheit: Wenn es um die Nutzung von Cloud-Technologie geht, gibt es für Unternehmen vielfältige Vorteile. „Die Unternehmen haben verstanden, dass Cloud-Computing eine grundlegende Technologie für das Geschäft von morgen ist“, sagt Axel Pols, Geschäftsführer von Bitkom Research. Cloud-Computing bezeichnet aus Sicht der Anwender die bedarfsgerechte Nutzung von IT-Leistungen wie beispielsweise Software, Speicherplatz oder Rechenleistung über Datennetze. Das Datennetz kann ein unternehmensinternes Intranet sein, das sogenannte Private-Cloud-Computing, oder das öffentliche Internet – dann spricht man vom Public-Cloud-Computing. Möglich ist auch eine Kombination von beidem – dann spricht man von einer Hybrid-Cloud. Und wenn man dann auch noch auf die Dienste unterschiedlicher Anbieter zurückgreift, spricht man von einer Multi-Cloud. Laut einer Bitkom-Research-Studie greift bereits jedes dritte Unternehmen hierzulande auf eine Multi-Cloud zurück.

Hybrid- beziehungsweise Multi-Clouds vereinen zwar die Vorteile von Public- und Private-Cloud-Systemen, stellen jedoch auch hohe Anforderungen an das Sicherheitsmanagement. Dabei ist die Public-Cloud-Komponente der Bitkom-Studie zufolge weniger anfällig für Sicherheitsvorfälle als die Cloud auf den unternehmenseigenen Servern: Gut ein Fünftel (22 Prozent) der Public-Cloud-Nutzer gibt an, dass es in den letzten zwölf Monaten zu Sicherheitsvorfällen in den von ihnen genutzten Cloud-Lösungen gekommen ist. Für weitere 36 Prozent bestand ein solcher Verdacht. Zum Vergleich: Von Sicherheitsvorfällen in der unternehmensinternen IT berichteten drei von zehn Unternehmen (28 Prozent), 40 Prozent hatten einen entsprechenden Verdacht. Die große Mehrheit verfügt über Sicherheitskonzepte für ihre Cloud-Lösungen: Gut drei Viertel der Cloud-Anwender (77 Prozent) geben dies an.

Verschlüsselung von Firmendaten

Gerade wenn in der Cloud weitverbreitete Programme wie etwa Microsoft 365 genutzt werden, ist ein solches Sicherheitskonzept unerlässlich. Denn die Gefahren durch Ransomware, Malware, Spam, Phishing oder Social Engineering sind nicht zu unterschätzen. „Kriminelle haben den Trend zur Cloudifizierung längst für sich erkannt und konzentrieren ihre Attacken auf Schwachstellen in den beliebtesten Produkten“, erklärt Thomas Uhlemann vom IT-Sicherheitshersteller ESET. „Während Microsoft-Exchange-Server zuletzt im März unter schwerem 0-day-Beschuss durch mehrere Gruppen standen, waren es vor allem im letzten Jahr die Microsoft-Share-Point-Instanzen, die Angreifer vehement fokussierten.“

Um solchen Gefahren zu begegnen, sollten die Unternehmen, die die entsprechenden Programme in der Cloud nutzen, auf umfassende Schutztechnologien setzen, rät Uhlemann. „Ein valides Sicherheitssystem startet mit perfekt abgesicherten Endpoints.“ Experten sprechen hier vom „Multi Secured Endpoint“, der mit Malwareschutz, Verschlüsselung und Multi-Faktor-Authentifizierung ausgerüstet ist. So haben Hacker kaum Angriffsfläche und können im Erfolgsfall mit erbeuteten Daten wenig anfangen. Zudem sollten alle Daten in den Cloudspeichern permanent auf Bedrohungen geprüft werden. Zu den wichtigsten Maßnahmen, um Cyberkriminellen das Handwerk zu legen, zählt zudem die wirksame Verschlüsselung von Unternehmens- und Kundendaten. Denn codierte Informationen können selbst bei einem erfolgreichen Angriff nicht zu Geld gemacht werden.

Wichtig sei zudem ein zeitgemäßer Zugang zur Cloud-Infrastruktur, sagt Uhlemann. „Professionelle Cloud-Sicherheitskonzepte sollten – egal bei welcher Organisationsgröße – auf Multi-Faktor-Authentifizierung setzen“, so der IT-Sicherheitsexperte.

IMPRESSUM

IT-Trends
Verlagsspezial der
Frankfurter Allgemeine Zeitung GmbH

Verantwortlich für den redaktionellen Inhalt:
Fazit Communication GmbH
Frankenallee 71–81, 60327 Frankfurt am Main

Geschäftsführung: Hannes Ludwig,
Jonas Grashey

Redaktion: Dirk Mewis,
Christina Lynn Dier (verantwortlich)

Anzeigen: Ingo Müller (verantwortlich) und
Jürgen Maukner, REPUBLIC Marketing &
Media Solutions GmbH, Mittelstraße 2–4,
10117 Berlin, www.republic.de

Weitere Angaben siehe Impressum
dieser Zeitung.