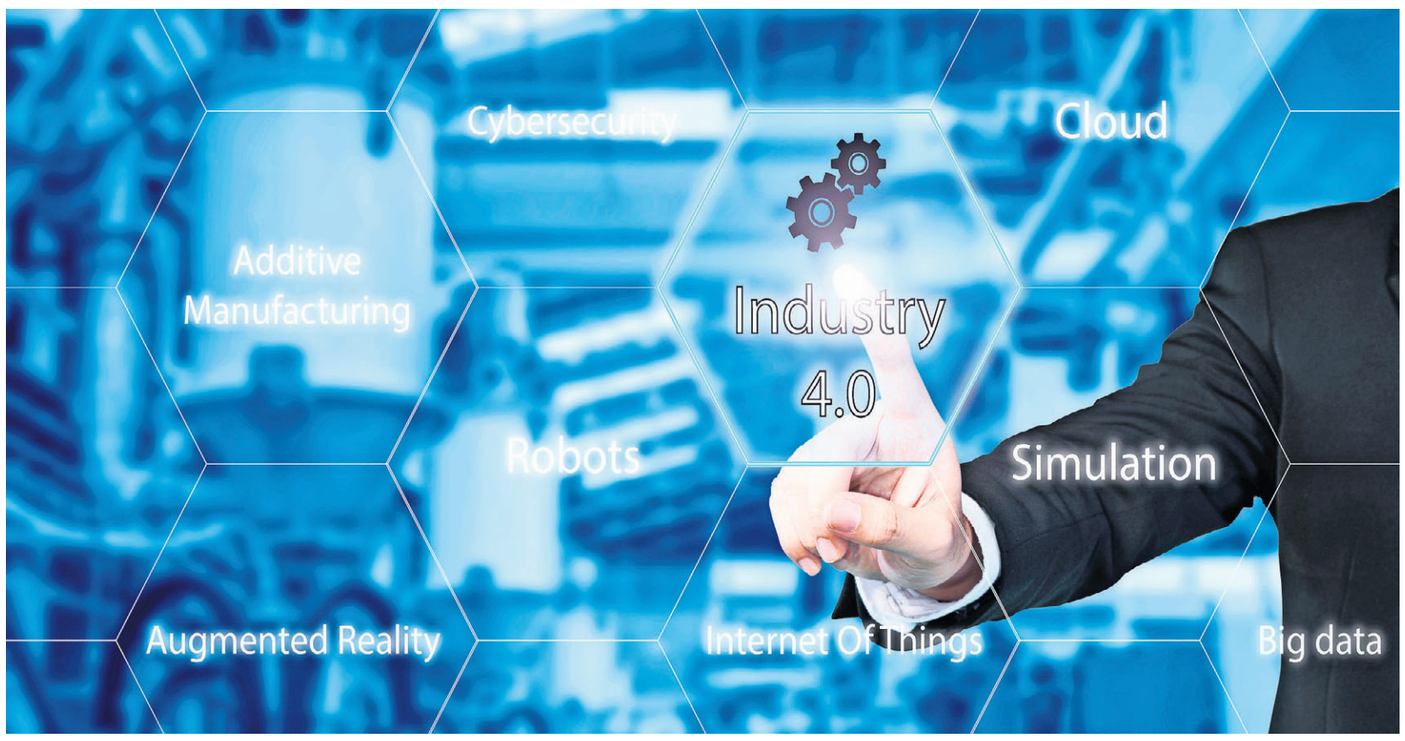
Viel Verkehr auf der Datenautobahn

Ausblick. Im Internet der Dinge müssen viele Daten verarbeitet werden. Doch Cloud Computing stößt an seine Grenzen. Edge- oder Fog-Systeme sollen helfen.



Je weiter die Vernetzung voranschreitet, desto mehr Daten müssen ausgewertet werden. Foto: Fotolia

Cloud Computing gilt als Schlüsseltechnologie für das Internet der Dinge. Schließlich ist nicht jedes Unternehmen in der Lage, die notwendigen technischen Kapazitäten – etwa für die Analyse von Daten – selbst bereitzustellen. Dafür auf Systeme aus der Wolke zurückzugreifen, statt sie im eigenen Haus zu installieren, ist daher naheliegend.

Doch je weiter die Vernetzung fortschreitet, desto näher kommt dieses Konzept an seine Grenzen. Eine Unmenge von Geräten sorgten für eine Masse an Daten, die an die Cloud übermittelt werden müssen, sagt Tadaaki Mataga, Analyst und Cloud-Computing-Experte beim Marktforschungshaus Gartner. Und diese verursachen viel Verkehr auf der Datenautobahn, der sich in hohen Netzwerkkosten bemerkbar macht.

Die Datenmenge lässt sich jedoch reduzieren, wenn ein Teil der Intelligenz näher an die Geräte rückt. Soll heißen, spezielle Mini-Recheneinheiten verarbeiten die Daten bereits im Voraus, bevor diese in die Cloud geschickt werden. Entweder sie selektieren die Informationen, damit sich nur noch die relevanten auf dem Weg in die Wolke machen. Oder sie analysieren diese gleich vor Ort.

Dieses Konzept hat einen Namen – oder eigentlich sogar zwei: Fog- beziehungsweise Edge-Computing. Schließlich ist Nebel – also Fog – auch nur eine Wolke, die sich näher am Boden befindet. Und die entsprechenden Systeme sitzen am Rande des Netzwerks – englisch: edge.

„Aus Edge, Fog und Cloud ergibt sich eine sehr flexible Architektur“, sagt Michael Stiller, wissenschaftlicher Mitarbeiter im Bereich Industriekommunikation beim Fraunhofer-Institut für Eingebettete Systeme und Kommunikationstechnik (ESK). Mit dieser könnten auch Anforderungen wie etwa die Latenz berücksichtigt werden. Damit meint er die Verzögerungszeit, mit der ein IT-System reagiert. Und diese ist gerade in der Fabrikhalle entscheidend. Wenn Maschinen im Mikrosekunden-Bereich reagieren müssen, reicht die Zeit nicht aus, um die Daten in ein Rechenzentrum in der Wolke zu übermitteln, diese dort zu analysieren und das Ergebnis zurückzuschicken. Da hilft es, wenn Informationen – zum Beispiel von Positionssensoren – vor Ort ausgewertet werden können.

Edge- beziehungsweise Fog-Computing bietet noch einen weiteren Vorteil. Da nicht alle Daten übermittelt werden, können besonders sensible Informationen innerhalb des eigenen Firmennetzes bleiben. Gerade für Unternehmen, die ihre Daten ungern in die Cloud geben, weil sie befürchten, dass diese dort ausspioniert werden könnten, stellt das neue Konzept somit eine Alternative dar.

SENSIBLE INFORMATIONEN

Streng genommen gibt es zwar einen feinen Unterschied zwischen den Begriffen Fog und Edge. Erstere sind quasi kleine Rechenzentren, die im Netzwerk eines Unternehmens sitzen und die Daten für den Weg in die Cloud vorbereiten. Bei Edge-Systemen dagegen bewegt sich die Intelligenz eine Ebene tiefer – zu den Geräten und ihren Sensoren, also dort, wo die Daten entstehen.

Viele Anbieter verwenden die Begriffe mittlerweile allerdings synonym. Und Hersteller, die solche Fog- oder Edge-Systeme entwickeln, gibt es bereits viele. Zum Beispiel haben IT-Größen wie HPE, Cisco oder Dell entsprechende Produkte in ihrem Programm. So bietet etwa HPE Geräte an, mit denen sich Fehler von Maschinen frühzeitig erkennen und korrigieren lassen sollen. Cisco stellt Technologien bereit, mit denen Unternehmen eigene Fog-Computing-Anwendungen entwickeln können. Dell hat gerade Systeme vorgestellt, die für die industrielle Automatisierung, den Einsatz im Transportwesen sowie für elektronische Werbetechnik konzipiert wurden.

Doch noch steht Edge- und Fog-Computing erst am Anfang seiner Entwicklung. Gartner-Analyst Mataga erwartet in der Industrie noch viele Diskussionen zu dem Thema.

Weitere Forschung ist ebenfalls gefragt. Laut Stiller vom Fraunhofer ESK werden Edge- und Fog-Systeme die Aufgaben der IT-Experten in den Unternehmen komplexer machen. Die Technik landschaft in den Fabriken ist durchaus zerklüftet – zum Beispiel sind viele verschiedene Maschinensteuerungen am Werk.

Die Herausforderung liegt nun darin, für diese verteilten Systeme ein einheitliches Programm zu schreiben, wie es für Edge- und Fog-Computing notwendig ist. Laut Stiller gibt es bereits viele Forschungsprojekte, die sich mit diesem Problem beschäftigen.

Für die intelligente Produktion der Zukunft könnte das Konzept trotzdem eine große Bedeutung haben. Er glaube, dass Fog-Computing ein grundlegendes Element für Industrie 4.0 darstellt, meint etwa Christian Schlögel, Technikchef des Roboterherstellers Kuka. Das Internet der Dinge starte „at the Edge“.

Markus Strehlitz

Phishing-Mail

Cyberkriminelle geben sich in Phishing-Mails gern als Provider, Paketdienst, Bank oder Behörde aus, um dem Empfänger sensible Daten wie Passwörter oder Kreditkartendaten zu entlocken. Doch solche Betrugsversuche lassen sich oft relativ leicht enttarnen, indem man die Absenderadresse analysiert, berichtet das Verbraucherschutz-Portal „Mobilsicher.de“. Kryptische Namen oder Zeichenfolgen in den E-Mail-Adressen wie „adebolajibolaji@xxx“oder „xxx@infymailz.info“ seien ein Alarmsignal. Solche Nachrichten sollte man gleich löschen. Wichtig ist auch, vorher keinesfalls auf Links oder Anhänge zu klicken. *dpa*

Digitalisierung

Die Digitalisierung ist laut einer Studie sowohl bei den Verbrauchern als auch in den Unternehmen in Deutschland angekommen. Eine große Mehrheit von 86 Prozent sei von ihrer Notwendigkeit überzeugt, ergab eine repräsentative Umfrage des Digitalverbands Bitkom. Sie glaubten, dass Deutschland nur so in wichtigen Branchen seine starke Stellung auf dem Weltmarkt verteidigen könne.

Eine Mehrheit von 56 Prozent der Bürger erwartet demnach, dass der Wohlstand in Deutschland durch die Digitalisierung zunehmen werde, zugleich gehen aber 33 Prozent vom Gegenteil aus. Auf der CeBIT in Hannover dreht sich in dieser Woche alles um die digitale Transformation und die Chancen, die sie für den Standort Deutschland eröffnet. *dpa*

IT-Gefahren frühzeitig erkennen

Cyber-Verbrechen. Security-Alarmanlage und Schutzhüllen für mobile Geräte können helfen.

Im vergangenen Jahr wurde jedes zweite deutsche Unternehmen mindestens einmal aus dem Netz attackiert, so der „Cyber Readiness Report 2017“ von Forrester Consulting. Gesamtschaden nach Schätzung des Branchenverbandes Bitkom: 51 Milliarden Euro. Zugenommen haben vor allem Cyber-Erpressungen. Und die Einschläge kommen näher: Der Sicherheitsanbieter Check Point hat 2400 aktive Schädlingsfamilien ausfindig gemacht, die IT-Systeme von Firmen angreifen.

IT-Security-Fachleute haben 2016 „das Ransomware-Jahr“ getauft. Internet-Gangster greifen einen oder mehrere Computer in einem Unternehmen an, legen sie lahm oder ziehen sensible Daten ab. Erst nach Zahlung einer Lösegeldsumme werde man die Rechner oder Daten wieder freigeben. Viele Betriebe gehen auf die Erpressung ein, weil die ihre Betriebsabläufe gewährleisten und sie Imageschäden vermeiden wollen.

In den nächsten Monaten wird laut

NEUE ANGRIFFSWELLE DROHT

Tim Berghoff, Sicherheitsexperte beim IT-Security-Unternehmen G Data, „eine neue Angriffswelle auf die deutsche Wirtschaft zurollen“. Vor allem der Mittelstand sei ein beliebtes Ziel für Digital-Verbrecher, „weil hier in vielen Betrieben die Schutzhüllen löcherig sind“. Auch die „Wolken“ der IT-Branche seien kein sicherer Aufbewahrungsort für sensible Informationen. Das mussten schon einige Unternehmen und Behörden feststellen, denen aus den nebligen Wolken, aus Rechnern irgendwo auf der Welt, Informationen abgezogen wurden. Deswegen bietet mittlerweile selbst US-Riese Microsoft eine Cloud („Azure“) mit Rechnern von T-Systems in Frankfurt und Magdeburg an, die den strengen deutschen Datenschutzbestimmungen und Compliance-Richtlinien entspricht.

Kriminelle agieren im Netz. Foto: Fotolia

IT-Sicherheits-Hersteller wie G Data bieten dafür eine speziell abgestimmte Managed-Endpoint-Security. Der Begriff steht für eine Lösung, unter die alle stationären und mobilen Geräte fallen, auch Tablets und Smartphones. Der Schutzschild an der Schnittstelle zur Rechnerwolke hält Trojaner- und Phishing-Attacken ab. Vorteil für den Betrieb, der ihn einsetzt: Er spart einen eigenen Server und Administrator und erhält regelmäßig die aktuelle Programmversion.

Wie können sich Unternehmen vor Erpressern aus dem Netz schützen? Tim Berghoff empfiehlt Unternehmen, „systematisch die eigene Sicherheitsstruktur zu analysieren und eine methodische Bedrohungs- und Schwachstellenanalyse vorzunehmen“. Die Mitarbeiter in vielen kleinen und mittelständischen Firmen kämen angesichts der zunehmenden Digitalisierung „nicht mehr hinterher“. Er fordert auch ein Umdenken in den Chefetagen. Neben Investitionen in Technik und Personal müsse IT-Sicherheit zur strategischen Aufgabe gemacht werden. „Und diese ist Chefsache.“ Seine Tipps: Starke Passwörter benutzen, nur wenigen Fachleuten Administrationsrechte gewähren, Updates und Patches umgehend einspielen. „Außerdem gehören regelmäßige Back-ups zum Einmaleins der Sicherheitsmaßnahmen ebenso wie das Anlegen von Wiederherstellungsroutinen.“ Selbstverständlich sei heute der Gebrauch von Antivirenprogrammen essenziell, aber ein wichtiger Baustein sei auch die Netzwerk-Gesundheit. Mithilfe integrierter Patch-Management-Lösung sollten Betriebe ihre Programme immer auf dem aktuellen Stand halten, um auch hier Schwachstellen für Angreifer zu schließen.

SCHWACHSTELLEN SCHLIESSEN

Dass Kontinuität wichtig ist, meint auch Dr. Christian Polster, Chefstratege beim Sicherheitsanbieter RadarServices. „Einmalige Aktionen werden keinen dauerhaften Schutz bieten. IT-Security ist ein Marathonlauf.“ Eine Cloud sei grundsätzlich zwar sicherer „als der Server im Keller“. Aber in der Wolke würden eben auch Daten vieler Unternehmen gesammelt. „Wenn man zum Nachbarn dünne Wände hat, nützen meine eigenen Sicherheitsmaßnahmen wenig.“ Ohnehin reichten Schutzmaßnahmen allein nicht. Polster plädiert für Security-Lösungen, die eine frühzeitige Erkennung von IT-Risiken und Cyber-Angriffen ermöglichen. „Mit statistischen Modellen findet man auch die Nadel im Heuhaufen.“ Stichwort: Big Data Cyber Security. Massen von Daten aus dem gesamten Netzwerk eines Unternehmens werden durch die „Sicherheits-Brille“ analysiert. „Am Ende bekommt der Kunde ein Cockpit, auf dem wir ihm zeigen, was er tun muss, um wieder sicher zu sein“, erklärt Polster. Seine Firma werde oft erst gerufen, „wenn der Hut schon brennt“. Meistens von Unternehmen, die keine eigenen IT-Security-Experten haben und sich nicht auf Dienstleister aus der amerikanischen oder israelischen Sicherheitsindustrie verlassen möchten. Polster: „Wir werden oft als Gegengewicht gesehen.“ *Anja Steinbuch*

Mit Netz und doppeltem Boden

Alternativ. Wer seine eigene Cloud nutzen möchte, braucht einen guten Internetanbieter.

Es ist verführerisch: Viele Firmen bieten PC- und Smartphone-Nutzern Cloud-Speicher an – also die Option, persönliche Daten auf ihren Servern zu lagern. Die Vorteile: Falls die eigene Hardware ausfällt, sind die Sicherungskopien gut geschützt in der Cloud. Zudem sind die Informationen von überall aus verfügbar.

Dennoch ist nicht jeder von den teils kostenlosen, teils kostenpflichtigen Cloud-Diensten überzeugt. Gerade von US-Anbietern fordern amerikanische Behörden immer wieder Zugriff auf Daten. Und regelmäßig machten Datendiebe bei Cloud-Diensten fette Beute.

Logische Folge: Wer Herr seiner Daten sein und bleiben will, richtet seinen eigenen Cloud-Server ein. Klingt kompliziert? Ist es nicht. Viele Modelle der verbreiteten Fritz-Box-Router fungieren als sogenanntes NAS – Network Attached Storage oder einfach Netz-Festplatte. Dazu hängt man eine externe Festplatte an einen der USB-Kontakte der Fritz-Box und richtet im Menü des Geräts die Zugriffsmöglichkeiten ein. Für Privatanwender reicht das meist, der Prozessor der Router des Berliner Herstellers AVM ist aber nicht der schnellste. Wer flinkeren Zugriff auf mehr Daten braucht, findet im Handel eigene NAS, die flotter agieren und beispielsweise in Echtzeit Videos für den Empfänger in besonders effiziente Formate wandeln – so kann man seine TV-Aufnahmen etwa auf dem Smartphone genießen.

Mindestens so wichtig wie die Technik des NAS ist die des heimischen Internetzugangs. Standard im Privathaushalt, aber auch vielen Kleinbetrieben sind ADSL-Anschlüsse. DSL steht für Digital Subscriber Line, also eine digitale Standleitung. Das A meint asymmetrisch. Heißt, diese Internetzugänge befördern Daten deutlich schneller zum Kunden als von ihm weg. Eine E-Mail mit einem größeren Dateianhang empfängt man also deutlich schneller als man sie verschickt. Fürs Protokoll: Auch die neueren, VDSL genannten Internetzugänge arbeiten asymmetrisch.

Wie in vielen Bereichen der Informationstechnik dominieren auch hier englische Begriffe. Der Downstream meint die Empfangsgeschwindigkeit, der Upstream die Sendegeschwindigkeit. Für ein gut von unterwegs aus nutzbares NAS ist der Upstream entscheidend. Aktuell offerieren die großen Anbieter oft 50 Megabit pro Sekunde (mbps) im Downstream und zehn im Upstream. Für eine sinnvolle Nutzung als Mini-Cloud-Server markieren zehn mbps die Untergrenze. Bei anderen Anbietern ist das Verhältnis aber auch mal ungünstiger. Hier gibt’s 100 mbps Downstream, aber nur fünf mbps Upstream.

Bei ADSL über die klassische Telefonleitung sichern sich die Telekommunikationsfirmen zwar mit den unscheinbaren Worten „bis zu“ gegen mögliche Schwankungen ab. Zwar leisten die Anschlüsse nicht überall das Maximum, aber die Übertragungsgeschwindigkeiten sind weitgehend konstant.

Anders sieht es aus, wenn ADSL von einem Breitbandkabelbetreiber stammt. Hier teilen sich alle an einem Knotenpunkt angeschlossenen Haushalte die verfügbare Bandbreite. Viele Nutzer dieser Zugangsart wissen aus leidiger Erfahrung: Abends, wenn viele Nutzer zu Hause sind und surfen wollen, geht die Geschwindigkeit in den Keller – nicht die besten Voraussetzungen, wenn ein NAS zuverlässig Daten liefern soll.

Praktisch alle privaten ADSL-Zugänge trennen nach 24 Stunden die Verbindung zum Anbieter. Beim normalen Surfen bekommt man davon so gut wie nie etwas mit. Die Router stellen die Verbindung zum Telekommunikationsunternehmen sofort wieder her. Dabei wechselt auch die IP-Adresse (Internet Protocol), also die Ziffernfolge, unter der Router und dahinterliegendes NAS aus dem Internet erreichbar sind. Die Zahlen werden zudem zufällig vergeben und sind ohne Weiteres von unterwegs aus nicht herauszufinden – und auch schwierig zu merken. Dynamische DNS-Dienste helfen. Hier kann man einen leicht zu behaltenden Namen („michael-mustermann.de“) vergeben, der Dienst leitet zur gerade aktuellen IP-Adresse weiter. Fritz-Box-Hersteller AVM bietet seinen Kunden einen entsprechenden Service an; andere Routerhersteller arbeiten mit ähnlichen kostenlosen oder -pflichtigen Dienstleistern zusammen.

An älteren Internetanschlüssen sind die IP-Adressen im sogenannten IPv4-Format. Dieser Adressraum ist weitgehend verbraucht; allen aktuell existierenden und in der nächsten Zeit erwartbaren Geräten mit Internetzugang lässt sich per IPv4 keine eindeutige Adresse zuweisen.

Standardmäßig erhalten Neukunden von Internetanbietern daher IP-Adressen aus dem wesentlich größeren Raum IPv6. Beim Surfen macht das keinen Unterschied, wer ein NAS aus dem Internet hinter einem IPv6-Anschluss erreichen will, hat aber ein Problem. Einfachste Lösung: Beim Neuanschluss nachfassen – auf Anfrage rücken manche Telekommunikationsunternehmen durchaus noch IPv4-Adressen raus.

Falls nicht, viele NAS-Hersteller unterhalten sogenannte Relais-Server, die zwischen IPv4 und IPv6 vermitteln; für die Käufer ihrer NAS ist der Dienst in der Regel kostenlos. Oft sind auch die dynamischen DNS-Dienste der Hersteller schon IPv6-fähig. In kniffeligen Fällen helfen Dienste wie sixxs.net oder – kostenpflichtig – feste-ip.net. *Karl-Gerhard Haas*