CLOUD-COMPUTING

Power aus der Wolke

Cloud-Computing ist auf dem Siegeszug. Vor allem Prozesse, die standardisiert sind oder viel Rechenleistung brauchen, werden ausgelagert. Doch Sicherheit und Geschwindigkeit können dagegensprechen.

VON MARKUS STREHLITZ

Zu Beginn wurde das Konzept kritisch beäugt – vor allem in Deutschland. Die Vorstellung, IT-Leistung aus einem Verbund von Großrechnern – einer Cloud – zu beziehen, die in Rechenzentren an irgendeinem Ort in der Welt stehen, ließ Firmenverantwortliche grübeln.

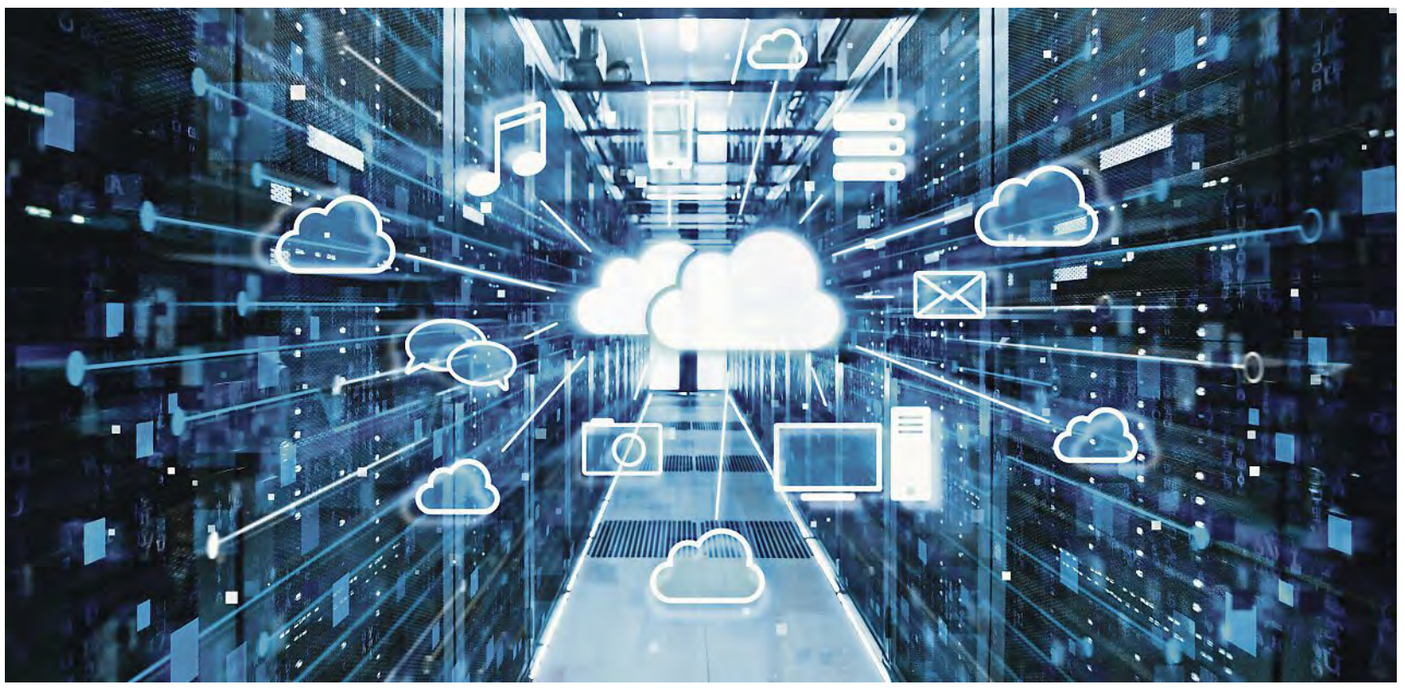
Doch mittlerweile hat sich das Cloud-Computing auch in Deutschland fest etabliert. Denn Unternehmen können so auf Mietbasis mit Informationstechnik arbeiten, statt in eigene Infrastruktur investieren zu müssen, die auch noch regelmäßig gewartet werden müsste. Das Angebot ist breit: Nutzer können in der Wolke auf reine Rechenpower zurückgreifen, um damit eigene Anwendungen zu entwickeln, oder sie können schon gefertigte Software-Funktionen beziehen.

Wer eine neue Technologie einführen möchte – etwa ein Softwaresystem für die Analyse von betriebswirtschaftlichen Daten – und die nötigen Investitionen dafür nicht aufbringen kann oder möchte, für den ist IT aus der Wolke eine attraktive Alternative.

SCHNELLER UND AGILER

Cloud-Computing macht auch flexibel. Ein Online-Shop beispielsweise, der zu bestimmten Zeiten im Jahr mehr Kundenanfragen als sonst üblich zu verarbeiten hat, kann sich kurzfristig die dafür nötige Rechen-Power hinzubuchen. „Viele Unternehmen möchten schneller und agiler werden, indem sie standardisierte Dienste und Funktionen nutzen, die von den Cloud-Anbietern technologisch immer auf dem neuesten Stand gehalten werden“, sagt Matthias Zacher, Analyst beim Marktforschungs- und Beratungshaus IDC. „Die Firmen sparen sich somit Anpassungen an die Hardware und Pflegeaufwand für die Anwendungen.“

Prozesse im Kundenbeziehungsmanagement und im Personalbereich seien klassische Einstiegsszenarien, so Zacher. Diese sind bereits sehr standardisiert und eignen sich daher besonders gut für das Cloud-Computing.



Komplexe Datenanalysen lassen sich in der Cloud einfacher abwickeln. Foto: Gorodenkoff/Adobe Stock

„Standardisierte Prozesse sind in der Cloud aufgrund von Skalierungseffekten häufig günstiger zu beziehen“, erklärt Patrick Schidler, der bei Microsoft das Marketing für das deutsche Cloud-Geschäft verantwortet. Cloud-Anbieter können Anwendungen für solche Tätigkeiten einmal entwickeln und dann einer Vielzahl von Firmen zur Verfügung stellen – zu entsprechend attraktiven Preisen.

Die Cloud biete außerdem enorme Vorteile, wenn es um große Datenmengen und hohe Rechenleistung gehe, meint Oliver Oursin, Vice President beim Cloud-Spezialist Salesforce. „Die dafür notwendigen Ressourcen können in der Cloud leichter und dynamischer zur Verfügung gestellt werden.“ Dazu zählen etwa komplexe Datenanalysen oder auch der Einsatz von Technologien für das maschinelle Lernen.

„Früher brauchte man beispielsweise schon hoch bezahlte Spezialisten, um grundlegende Lösungen für das Internet der Dinge oder künstliche Intelligenz aufzubauen“, berichtet Schidler. Heute könnten solche Dienste quasi von jedem Mitarbeiter schlüsselfertig aus der Cloud bezogen werden.

Laut Analyst Zacher wandern fast alle Prozesse in die Wolke. Selbst Sicherheit ist mittlerweile ein Argument für diese Art der IT-Nutzung. „Große Cloud-Anbieter haben sehr gute Sicherheitsteams und können ein Schutz-Level gewährleisten, das sich gerade kleine und mittlere Unternehmen nicht immer leisten können“, sagt Oursin. Und Microsoft-Mann Schidler fügt hinzu: „Die meisten Vorgaben des Datenschutzes oder Steuerrechts sowie viele industrie- oder unternehmensspezifische Vorgaben lassen sich heute in der Cloud abbilden.“

In bestimmten Fällen kann der Sicherheitsaspekt aber nach wie vor auch gegen Cloud-Computing sprechen. Das gelte etwa für Daten, die aufgrund ihrer Wichtigkeit auch innerhalb des Unternehmens physikalisch von anderen getrennt sind und in separaten Netzwerken gehalten werden, heißt es vonseiten des Cloud-Anbieters Servicenow. Diese fänden in der Regel in der Cloud nicht die entsprechenden Bedingungen vor.

MANGELNDE GESCHWINDIGKEIT

Ein weiteres Argument gegen die Cloud kann auch die mangelnde Geschwindigkeit sein. Manche Geschäftsprozesse benötigen extrem schnelle Rückmeldungen. Bestimmte Sensordaten von Produktionsmaschinen müssen im Mikrosekunden-Bereich verarbeitet werden. In diesem Fall reicht die Zeit meist nicht aus, um die Daten in ein Rechenzentrum in der Wolke zu übermitteln, diese dort dann zu analysieren und das Ergebnis zurückzuschicken. Häufig bietet das vorhandene Netz auch einfach nicht die notwendige Geschwindigkeit und Bandbreite. Die mangelhafte Netzabdeckung ist aktuell gerade in Deutschland ein viel diskutiertes Thema.

Einige Cloud-Anbieter haben auf diese Anforderungen aber schon reagiert. Sie stellen spezielle Mini-Recheneinheiten bereit, die Daten schon im Unternehmen vor Ort verarbeiten oder nur noch einen Teil davon in die Wolke schicken. Das Schlagwort lautet Edge-Computing, weil die entsprechenden Systeme am Rande des Netzwerks – englisch: Edge – stehen. So schreitet der Siegeszug der Cloud-Technik weiter voran.

» impressum

Produktion: STZW Sonderthemen
Anzeigen: Jürgen Maukner

Was tun, wenn Hacker Erfolg hatten?

Immer öfter werden Betriebe digital angegriffen. Laut Bitkom summierten sich die Schäden in den vergangenen zwei Jahren allein bei deutschen Industrieunternehmen auf mehr als 43 Milliarden Euro.

VON JÜRGEN HOFFMANN

Der Angriff kam schnell und überraschend. Anfang September drangen Cyber-Kriminelle in die IT-Architektur der Landesmesse Stuttgart ein und legten den kompletten E-Mail-Verkehr lahm. Auch die digital verbundenen städtischen Töchter Stadtwerke, in.Stuttgart und Stuttgart-Marketing wurden von den Tätern, die Lösegeld verlangten, in Geiselhaft genommen. Bei Armin Dellnitz, Geschäftsführer der Stuttgart-Marketing, entstand „ein Gefühl einer Ohnmacht“. Nicht der erste Fall. Auch das Stuttgarter Staatstheater, die Tübinger Buchhandlungskette Osiander und Tausende Firmen in ganz Deutschland sind schon Opfer solcher Angriffe geworden. Laut dem Digitalverband Bitkom verursachten Hacker-Überfälle in den vergangenen zwei Jahren allein bei Industrieunternehmen in Deutschland Schäden von mehr als 43 Milliarden Euro.

Was tun, wenn man merkt, dass ein Cyberangriff erfolgreich war? Zunächst gilt: kühlen Kopf bewahren! „Nach dem Erkennen eines Angriffs ist das Wichtigste, dass man verhindert, dass die Schadsoftware sich im betrieblichen Kommunikationsnetz weiterverbreitet“, betont Tim Berghoff vom IT-Security-Unternehmen G Data. Er empfiehlt Firmen, einen „Erste-Maßnahmen“-Katalog mit den drei, vier wichtigsten Schritten aufzustellen und an jeden Rechner zu hängen: „Wie im Fall eines Brandes muss jeder Mitarbeiter auch bei einer Cyberattacke wissen, was er zu tun hat.“ Auf der Notfallliste steht zum Beispiel: 1. Netzwerkstecker des Rechners ziehen! 2. Kabel an den Bildschirm kleben, damit jeder sieht, dass der Rechner vom Netz ist! 3. Notrufnummer der IT-Abteilung wählen! „Die Anweisungen müssen einfach und unmissverständlich sein“, betont der Security-Experte. Er warnt davor, dass User selbst aktiv werden und versuchen, ein Problem zu lösen: „Sie verwischen dabei oft unbeabsichtigt Spuren, die wertvoll für Forensiker sein können.“

KLARE ANWEISUNGEN GEBEN

Eine Frage, die im Vorfeld beantwortet werden sollte: Wer aus der IT-Abteilung kann den unternehmensweiten IT-Notfall ausrufen und das Notfallprotokoll in Gang setzen? Berghoff: „Diese Aufgabe müssen mehrere Mitarbeiter erfüllen können, sonst drohen im Ernstfall Verzögerungen.“ Außerdem brauche jede Firma eine Liste mit Kriterien, anhand derer der zuständige Mitarbeiter klar erkennt, wann ein solcher Notfall vorliegt. „So hat er die Gewissheit, das Richtige zu tun, wenn er mit der Umsetzung des Notfallplan beginnt.“

Die Datenschutz-Grundverordnung verlangt, dass Unternehmen Überfälle aus dem Netz den Aufsichtsbehörden melden. Empfohlen wird außerdem bei Hacker-Angriffen, möglichst frühzeitig die Zentrale Ansprechstelle Cybercrime der Polizei hinzuziehen. Apropos Polizei: Die rät dringend, Erpressungen von Cyber-Kriminellen nicht nachzugeben. Erstens können auch die Täter oft nichts mehr reparieren. Zweitens würden die Täter durch Lösegeldzahlungen ermutigt, es bei der Firma ein zweites oder drittes Mal zu probieren.

Wer der Cyberattacke etwas Positives abgewinnen will, sollte versuchen, aus diesem Ereignis zu lernen: Analysieren, die richtigen Schlüsse ziehen und dann Maßnahmen ergreifen, die eine Wiederholung ausschließen. Das kostet Zeit und Geld. Aber jede Investition in IT-Sicherheit ist günstiger, als nichts zu tun und nach dem nächsten Angriff erneut Schäden beheben zu müssen.

Kriminelle blockierten den E-Mail-Verkehr der Messe. Foto: R. Halbe/Messe Stuttgart

» INFO

Eine Versicherung gegen Cyberangriffe kostet kein Vermögen. Signal Iduna beispielsweise bietet eine Police schon ab 20,82 Euro im Monat an. Bereichsleiter Dr. Andreas Reinhold: „Firmenchefs wird allmählich klar, dass eine Cyberversicherung ein wichtiger Teil des betrieblichen Risikomanagements ist.“ Die Versicherungsgesellschaft hat „Maßanzüge“ wie den „Digitalen Schutzschild“ für kleine und mittlere Firmen geschneidert. Abgedeckt sind Informationssicherheitsverletzungen und daraus entstandene Betriebsunterbrechungen. Neben der Übernahme von Kosten beispielsweise für IT-Forensiker, die Art und Umfang des Schadens beurteilen und beheben, stellt Signal Iduna über die IT-Security-Firma Perseus rund um die Uhr eine Notfall-Hotline zur Verfügung.

Jürgen Hoffmann

Wolken für alle Computernutzer

Nicht nur Unternehmen profitieren von Cloud-Diensten. Auch Privatanwender haben einen Nutzen.

VON KARL-GERHARD HAAS

Die aktuellen Versionen der Betriebssysteme von Apple, Google und Microsoft drängen bei ihrer Installation Nutzer regelrecht zu den Cloud-Angeboten der Hersteller. Klar: Elektronische Post oder Kurznachrichtendienste wie Whatsapp funktionieren ohne Internet nicht. Aber die Softwarefirmen ködern auch mit kostenlosem oder günstigen Speicherplatz auf ihren Servern. Oft gibt’s auch gleich Cloud-Programme dazu, um die typischen Bürodokumente, also Texte, Tabellen oder Präsentationen zu erstellen und zu bearbeiten. Aber soll man als privater Computer- oder Smartphonenutzer auf diese Dienste setzen? Jein, es kommt drauf an.

KOPIEN LOKAL SPEICHERN

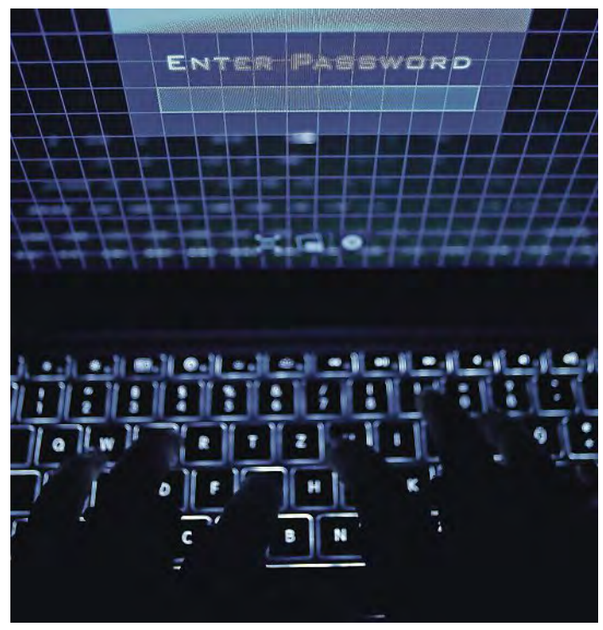
Speicher in der Cloud zu nutzen ist grundsätzlich nicht verkehrt. Egal, wo man ist und an welchem Gerät man gerade arbeitet – man hat Zugriff auf seine Daten. Meistens jedenfalls, denn bei allen internetbasierten Dienstleistungen muss man sich darüber im Klaren sein, dass sie eben eine funktionierende Internetverbindung voraussetzen. Funkloch, Störung beim Internetprovider, der heimische Router hat gerade seinen Geist aufgegeben, technische Probleme beim Cloud-Dienstleister – schon kommt man nicht an seine Unterlagen ran. Es ist also in jedem Falle ratsam, Kopien seiner Dokumente und Dateien auf einem lokal verfügbaren Speichermedium zu halten. Es hängt vom jeweils verfügbaren Gerät und dessen Möglichkeiten ab, ob man die klassische Festplatte, USB-Stick oder eine Speicherkarte dafür wählt.

Anbieter von Cloud-Speicher sind bisher nicht durch schlampigen Datenschutz aufgefallen – wenn es in der Vergangenheit Skandälchen gab, weil etwa hüllenlose Selbstporträts Prominenter auftauchten, lag dies in der Regel daran, dass die Herrschaften ihre Fleischbeschau mit einfach zu erratenden Passwörtern „sicherten“ oder Spanner ihnen mit gefälschten E-Mails die Passwörter entlockten. Wer die Dienste von US-Anbietern nutzt, muss allerdings damit rechnen, dass sich amerikanische Behörden Zugriff auf Clouddaten verschaffen, wenn sie das für nötig erachten.

Letztlich sind diese Betrachtungen akademischer Natur: Wer vertrauliche Daten ohne eigene Verschlüsselung bei Dritten lagert, spielt immer mit dem Feuer. Nutzt man nur gelegentlich die Cloud als zusätzliche Sicherung, kann man beispielsweise die zu speichernden Daten mit dem für viele Betriebssysteme kostenlos verfügbaren Programm 7-zip (7-zip.org) packen und dabei ein Passwort vergeben. Wenn das sicher ist, also aus einer nicht erratbaren und ausreichend langen Ziffern- und Buchstabenkombination besteht, sind die Daten vor neugierigen Blicken geschützt.

Andere Möglichkeit: Man installiert das Programm Cryptomator (cryptomator.org), das ebenfalls für alle Arbeitsplatz- und Smartphone-Betriebssysteme verfügbar ist. Einmal eingerichtet verschlüsselt dies alle in die Cloud gehenden Daten ohne Zutun des Nutzers. Diese Vorgehensweise ist sinnvoll, wenn man mit vielen einzelnen Dateien hantiert. Allerdings: Will man Freunden oder Kollegen Zugang zu den Daten erlauben, müssen diese ebenfalls Cryptomator installieren.

Ähnliche Überlegungen wie für Cloud-Speicher gelten für Cloud-Arbeitsprogramme. Wer seine Texte mit Diensten wie Google Docs erstellt, sollte einfach realisieren, dass der Anbieter mitlesen kann – für vertrauliche Inhalte sicher nicht die klügste Wahl.



Gute Passwörter bestehen aus langen Ziffern- und Buchstabenkombinationen. Foto: Oliver Berg/dpa-tmn

Die Cloud auf einen Blick

Zahlreiche Fachbegriffe tauchen im Kontext von Cloud-Computing auf.

VON ANJA STEINBUCH

Wer Cloud-Computing verstehen will, sollte die wichtigsten Begriffe rund um das Thema kennen.

Multi Cloud
„Ein Multi-Cloud-Modell setzt auf Cloud-Services verschiedener Anbieter, um unterschiedliche Aufgaben zu erledigen“, erklärt Sebastian Stein, Technischer Vertrieb beim Cloud-Security-Anbieter Zscaler in München. Während Unternehmen sich früher zwischen „Cloud oder nicht Cloud“ entscheiden mussten, stehen heute für verschiedene Bedürfnisse unterschiedliche Angebote von „Wolken“ zur Verfügung. „Bei einem auf Zero Trust basierten Ansatz lässt sich genau festlegen, welcher Mitarbeiter oder Dienstleister auf welche Anwendung zugreift – ein entscheidender Sicherheitsfaktor“, resümiert Stein. Wie man seine Multi Cloud vor Angriffen schützt, ist Thema auf dem Cybersecurity-Summit „Command Control“ Anfang März in München.

Cloud Hosting
Rechenzentren sind out. Daten gehen in die Cloud. Das nennt man Cloud Hosting. Vorteil: Verschiedene Speicher-Modelle sind möglich. Ähnlich wie ein Rechenzentrum funktionieren Private Clouds. Hier hat das Unternehmen seine eigene Server-Umgebung mit eigener Infrastruktur – ideal für Firmen, die ihre Speicher- und Rechenleistung stellenweise deckeln müssen und ein geschlossenes und sichereres System brauchen. Außerdem gibt es Public Clouds. Sie sind flexibel und skalierbar.

Blockchain
Die Blockchain ist eine transparente Datenbank. Beispiel: Der digitale Kontoauszug verzeichnet alle Einzelheiten einer Transaktion und ist für die Mitglieder des Netzwerks einsehbar. Durch dieses Verfahren ermöglicht die Blockchain Transparenz zwischen den einzelnen Transaktionspartnern. Bisher war es ein sogenanntes Hauptbuch, das für die Verwaltung aller Einzelheiten einer Transaktion zuständig war. Jetzt tritt die transparente Datenbank an seine Stelle.

Edge Computing
Edge Computing ist eine verteilte, offene IT-Architektur, die sich durch dezentralisierte Verarbeitungsleistung auszeichnet und die Grundlagen für Mobile Computing und das Internet der Dinge schafft. Die Daten werden von einem Gerät oder von einem lokalen Server verarbeitet und nicht an ein Rechenzentrum übertragen. Das macht die Daten schneller und deren Verarbeitung in Echtzeit möglich. Autonome Fahrzeuge brauchen das, Produktionsabläufe werden schneller.

Robotic Process Automation (RPA)
Roboter können sehr unterschiedliche Formen haben. Software-Roboter zum Beispiel verschieben Dateien und Ordner, kopieren Kundendaten aus dem CRM-System in Rechnungen, füllen Formulare aus oder antworten auf einfache Kundenanfragen – das nennt man Robotic Process Automation. Basierend auf Algorithmen der Künstlichen Intelligenz werden sie die Einsatzmöglichkeiten von Robotic Process Automation erheblich erweitern. Software-Roboter können Wartungsaufträge bearbeiten.

Managed Services
Bei den Managed Services handelt es sich um Dienstleistungen, die im Auftrag eines Unternehmens von einem Managed Services Provider (MSP) erbracht werden. Das Unternehmen überträgt dem Provider wiederkehrende IT-Services, um selbst effizienter und wirtschaftlicher zu arbeiten. Mögliche Services können Netzwerkdienstleistungen, Anwendungen, Monitoring, Storage oder Security-Services sein. Umfang, Art und Qualität der zu erbringenden Leistungen sind im Vorfeld exakt definiert und zwischen dem Unternehmen und Provider abgestimmt.

Künstliche Intelligenz (KI)
„Künstliche Intelligenz ist im Jahr 2019 keine Zukunftsvision mehr, sondern handfeste Realität“, sagt Bruno Messmer, Leiter Digital Strategy & Transformation Consulting bei DXC Technology. Sprachagenten wie Siri, Cortana oder Alexa durchdringen bereits den Alltag. Sie haben ihr Wissen dank KI. Die smarten Assistenten spielen die Lieblingsmusik ihres Besitzers, machen Restaurantvorschläge, empfehlen Filme, erkennen die schnellste Route zum Ziel und steuern einen Wagen besser in eine Parklücke als der Fahrer.

Um Probleme zu vermeiden, sollte im Vorfeld vertraglich auch festgehalten werden, was mit den Daten passiert.
Foto: ilkercelik/Adobe Stock

Am Anfang stehen die Daten

Wer Cloud-Dienste nutzen möchte, sollte unter anderem die Nutzungsrechte detailliert festhalten.

VON MARKUS STREHLITZ

Cloud-Computing lässt sich für eine Vielzahl von Anwendungen nutzen. Nahezu jedes Software-System steht auch als Internetdienst bereit und muss nicht im eigenen Unternehmen installiert werden.

Aber unabhängig davon, wofür die Cloud verwendet wird – fast immer strömen Daten in die Wolke. So stellen zum Beispiel viele Dienstleister mittlerweile ein Angebot zur Verfügung, mit dem sich Daten von Produktionsmaschinen analysieren lassen. Technische Probleme der Anlagen sollen sich auf diese Weise frühzeitig erkennen lassen, kostspielige Ausfälle könnten verhindert werden. Die Branche spricht von Predictive Maintenance – also vorausschauender Wartung.

INFORMATIONSSCHATZ-DATEN

Doch dafür muss das Unternehmen die Daten seiner Maschinen zur Verfügung stellen – und wissen, dass sich aus diesen häufig noch viel mehr ablesen lässt. „Ein IT-Spezialist eines großen Konzerns berichtete mir kürzlich von dem Predictive-Maintenance-Angebot eines Maschinenherstellers. Nachdem er sich dieses genauer angesehen hatte, war klar: Der Maschinenbauer erhält damit vollen Einblick in die Produktion“, sagt IT-Anwalt Andreas Leupold.

In den Daten aus der Fertigung oder aus betriebswirtschaftlichen Systemen liegt ein wahrer Informationsschatz. Und wer Zugriff auf die Daten hat, ist theoretisch in der Lage, diesen zu heben. Das gilt auch für einen Cloud-Dienstleister. Ohne vorherige vertragliche Vereinbarungen hat der Nutzer des Cloud-Services keine Möglichkeit, dies zu verhindern. Der Grund: Anders als an physischen Objekten – der Jurist spricht von körperlichen Sachen – kann an Daten kein Eigentum erworben werden.

Das heißt: Unternehmen müssen dies in den Vereinbarungen mit dem Cloud-Anbieter beachten. In den entsprechenden Verträgen muss genau definiert werden, welche Daten betroffen sind und was mit diesen geschehen darf. „Es ist im Einzelnen zu spezifizieren, welche Nutzungsrechte dem Vertragspartner eingeräumt werden“, erklärt Leupold.

Das wiederum bedeutet: Bevor Firmen in die IT-Wolke starten, brauchen sie einen Überblick, welche Daten nach außen gelangen. Und sie müssen wissen, wie schutzbedürftig die jeweiligen Datenarten sind. Die Daten selbst sind schließlich nur die Grundlage. Die Informationen, die aus ihnen gewonnen werden, können Wissen enthalten, das nicht an Dritte gelangen sollte.

Daraus ergibt sich, dass nicht alle Informationen den gleichen Schutz erfordern. Leupold empfiehlt, Schutzklassen zu bilden, die unterschiedlicher vertraglicher Absicherung bedürfen.

Hinzu kommt: Es reicht nicht, sensible Informationen wie zum Beispiel Know-how aus der Fertigung als geheim zu bezeichnen. Der Gesetzgeber fordert, dass diese auch durch angemessene technische Maßnahmen vor einer Offenlegung geschützt werden.

Eine Firma, die einen Cloud-Dienst nutzt, kann also die Verantwortung in diesem Punkt nicht einfach an den Anbieter abgeben. Dem Unternehmen sollte daran gelegen sein, dass die Daten in der Wolke ausreichend geschützt sind – schon allein um sicher zu sein, dass die damit verknüpften Informationen den gesetzlichen Anforderungen an ein schützenswertes Geschäftsgeheimnis entsprechen.

GESCHÄFTSGEHEIMNISSE SCHÜTZEN

Es gibt aber noch einen weiteren Grund, warum sich Firmen ihre Daten genau anschauen sollten, bevor der Schritt in die Cloud gewagt wird. Erkenntnisse können nur dann gewonnen werden, wenn auch die Qualität der Daten stimmt. Somit ist also vorab zum Beispiel zu klären: Sind die Daten aktuell? Sind sie vollständig? Gibt es Dubletten? Gerade in Bezug auf Stammdaten sind dies sehr entscheidende Fragen. Und nur wenn diese beantwortet sind, kann ein Unternehmen auch darauf hoffen, dass etwa das Auslagern von betriebswirtschaftlichen Software-Funktionen einen Nutzen bringt.

Die Vorbereitungen, die beim Thema Daten getroffen werden müssen, sollten Unternehmen aber nicht generell vom Cloud-Computing abhalten. Zumindest was die rechtliche Komplexität betrifft, plädiert Anwalt Leupold für Gelassenheit. Grundsätzlich sei das Erstellen von Verträgen, welche die Datennutzung regeln, zwar nicht trivial, aber die Zeit, die dafür aufgebracht werden muss, sei „gut investiert“.

» INFO

Anders als an körperlichen Sachen kann an Daten noch kein Eigentum erworben werden. IT-Anwalt Andreas Leupold sieht diesbezüglich Nachholbedarf auf Gesetzesseite. „Daten bilden die Grundlage, um daraus einen Wissensschatz zu heben. Daher brauchen wir in der einen oder anderen Form eine Zuordnung der Daten.“ Laut Leupold liegt ein Vorschlag für die Einführung eines Datenerzeugerrechtes auf europäischer Ebene momentan auf Eis. „Es wäre aber wünschenswert für die Wirtschaft, wenn man eine Lösung finden würde – auch wenn es Widerstände gibt.“
Markus Strehlitz