Prognosen für 2020: Cloud, vernetzte Autos und Medizin sowie Cybersicherheit – das sind die Trends

17. Dezember 2019

Peter Galvin | Chief Strategy Officer
Mehr über diesen Autor >

Autonomes Fahren. Cloud-Computing. Vernetzte Medizin. Datenschutzverletzungen.

Diese Erfindungen, Anwendungsfälle und Herausforderungen sind seit Jahren wichtige technologische Themen. Und in all diesen Bereichen erwarten uns im kommenden Jahr erhebliche Veränderungen.

Die voraussichtlichen Entwicklungen werden durch eine Kombination aus neueren Erkenntnissen, technologischen Fortschritten und besserer Organisation vorangetrieben. Die zu erwartenden Auswirkungen sind – fast immer – positiv.

Was wird sich 2020 also in diesen wichtigen Bereichen tun? Hier sind meine Prognosen.

Der Weg hin zum autonomen Fahren wird immer länger, und die Einschränkungen nehmen zu.

Wer glaubt, dass sich autonomes Fahren nach Science Fiction anhört, ist in guter Gesellschaft. Viele von uns halten autonomes Fahren immer noch für eine ziemlich ausgefallene Idee. Und in gewisser Weise ist es das auch.

Wie wir alle wissen, gibt es bereits heute selbstfahrende Fahrzeuge. Das bedeutet jedoch nicht, dass sie in absehbarer Zeit das Straßenbild beherrschen werden. Vielmehr werden die meisten autonomen Fahrzeuge, die erfolgreich auf den Markt kommen, einen engen Anwendungsbereich und eine geringe Reichweite haben.

Die große Herausforderung liegt darin, ein Konzept zu finden, wie selbstfahrende Fahrzeuge sicher in den Straßenverkehr integriert werden können. Dass sich dabei Hindernisse auftun, ist nur verständlich. Tatsächlich sind die Probleme, die das autonome Fahren birgt, viel größer als erwartet. Dazu gehören auch tödliche Unfälle.

Daher sind wir derzeit weiter vom autonomen Fahren entfernt als ursprünglich prognostiziert. Aus diesem Grund lässt sich ein Umdenken bei der möglichen Nutzung selbstfahrender Fahrzeuge erkennen, die sich auf bestimmte Routen, Geschwindigkeiten sowie festgelegte Entfernungen beschränken wird. Wie ein Ski-Shuttle werden sie nur auf einer festgelegten Strecke zum Einsatz kommen und nur eine begrenzte Anzahl von Aufgaben haben.

Der Bumerangeffekt fördert die Akzeptanz von Multi-Cloud-Anwendungen mit mehreren Bereitstellungsmodellen

Die IDC schätzt, dass in diesem Jahr weltweit 229 Milliarden Dollar für öffentliche Clouds ausgegeben werden und diese Zahl 2023 sogar auf fast 500 Milliarden Dollar steigen wird. Eine Umfrage von Gartner zeigt, dass 81 % der Benutzer öffentlicher Clouds mit zwei oder mehr Anbietern arbeiten. Aber die Firma rät Unternehmen davon ab, direkt von On-Premises zu Multi-Cloud zu wechseln. Feine Unterschiede machen es schwierig, Dienste auf mehrere Plattformen zu verteilen, so dass Unternehmen es langsam angehen sollten, um ihren Mitarbeitern genügend Einarbeitungszeit zu geben.

Trotz aller Herausforderungen erwarte ich, dass sich Multi-Cloud-Umgebungen mehr und mehr durchsetzen werden. Aber ich glaube auch, dass 2020 ein stärkerer Fokus auf Technologien gelegt werden wird, die neben öffentlichen auch auf lokale und private Cloud-Umgebungen ausgerichtet sind. Wir können das auf den Bumerangeffekt zurückführen.

Noch vor wenigen Jahren planten viele Unternehmen, zu 100 % in die öffentliche Cloud zu wechseln. Im Einzelfall haben diese Unternehmen auch tatsächlich bestimmte Anwendungen in die Cloud verlagert. Viele von ihnen haben dabei festgestellt, dass die öffentliche Cloud nicht immer alle ihre Anforderungen erfüllt. Sicherheitsprobleme, das Umschreiben von Anwendungen und weitere Herausforderungen haben zu dieser Erkenntnis geführt. Infolgedessen wurden bestimmte Anwendungen wieder On-Premises bereitgestellt.

Unternehmen setzen heutzutage zunehmend auf Multi-Cloud-Umgebungen mit mehreren Bereitstellungsmodellen. Ob On-Premises oder in der Cloud – sie stellen Anwendungen bereit, die die beste Technologie bieten und sicher sind.

Ich bin der Meinung, dass sich zunehmend Geschäftsanwendungen durchsetzen werden, die Cloud-Umgebungen imitieren – auch wenn sie technisch gesehen eigentlich nicht unter den Begriff öffentliche Cloud fallen. Unternehmen werden ihre Infrastruktur und Architektur so organisieren, dass sie Anwendungen aus- und erweitern sowie Arbeitslasten erhöhen und senken können. Diese Umgebungen werden der öffentlichen Cloud auffallend ähnlich sein, aber On-Premises oder in einer privaten Cloud bereitgestellt werden.

Vernetzte Medizin sorgt für mehr Hausbesuche

Vor ein paar Jahren veröffentlichte WIRED einen Artikel mit dem Titel „Healthcare 2020: The e-Doctor Will See You Now“. Dieser beschäftigte sich mit dem wahrscheinlichen Rückgang von papierbasierten Prozessen in der Medizin. Der Artikel ging davon aus, dass Patienten mit der Zeit mehr Einfluss auf ihre Gesundheitsversorgung ausüben würden. Ferner wurde

bemerkt, dass Patienten mithilfe von Wearables ihre Gesundheit überall und jederzeit überwachen können.

Diese Trends zeigen sich teilweise schon heute. Es wird erwartet, dass sie sich im kommenden Jahr noch verstärkt durchsetzen werden.

2020 werden große medizinische Geräte, wie z. B. Atemgeräte, die bisher nur in medizinischen Einrichtungen verfügbar waren, ihren Platz in Haushalten finden. Die Geräte werden kleiner, mit dem Internet verbunden und für den Heimgebrauch verfügbar sein, indem sie an das Netz angeschlossen sind. Die Möglichkeit, diese Geräte zu Hause einzusetzen, wird sowohl der medizinischen Industrie als auch den Verbrauchern Zeit und Geld sparen. Außerdem können so die Gesundheit verbessert und Leben gerettet werden.

Datenschutzverletzungen sind weiterhin eine große Herausforderung

Durch immer mehr vernetzte Geräte und die Migration personenbezogener Daten in verbundene Systeme wird das Risiko weiter erhöht. Daher werden wir 2020 genauso viele – wenn nicht sogar mehr – Datenschutzverletzungen erleben wie 2019.

Kriminelle haben erkannt, dass mit Datenverletzungen viel Geld gemacht werden kann. Infolgedessen geht die Entwicklung weg von einzelnen Hackern hin zu organisierten kriminellen Zusammenschlüssen, die auf der Suche nach personenbezogenen Daten sind.

Medizinische Daten, die eine wertvolle Fundgrube an Informationen darstellen, sind für Hacker besonders attraktiv. Berichten zufolge können vollständige medizinische Aufzeichnungen im Darknet bis zu 1.000 Dollar einbringen. Das ist viel mehr als nur Kreditkarteninformationen oder Sozialversicherungsnummern allein. Unbefugte können an medizinische Daten gelangen, indem sie tragbare und implantierte Geräte hacken, um mit den elektronischen Gesundheitsdaten der Patienten Zugang zu einem Gesundheitssystem zu erlangen.

Es gibt verschiedene andere Faktoren, die das allgemeine Problem Cybersicherheit noch verschärfen. Dazu gehören menschliches Versagen und Unternehmen, die Schwierigkeiten haben, das Gleichgewicht zwischen „ausreichender“ und „zu viel“ Sicherheit zu finden.

Unternehmen benötigen Sicherheits- und Datenschutzkontrollen, aber nur in einem Maße, das die Verbraucher nicht abschreckt. Die Herausforderung ist, hier das richtige Gleichgewicht zu finden. Unternehmen, die zu wenig auf Sicherheit setzen, werden sich im kommenden Jahr verstärkt mit Datenschutzverletzungen auseinandersetzen müssen.

Weitere Informationen über unsere Sicherheitslösungen finden Sie auf der Website von Entrust. Folgen Sie uns auch auf Twitter, LinkedIn und Facebook.