STORMSHIELD

MEINUNGEN

WAS WÄRE, WENN CLOUD COMPUTING UNUMGÄNGLICH GEWORDEN WÄRE?

Victor Poitevin
Editorial & Digital Manager, Stormshield

In einer immer kollaborativeren und interoperableren Welt wächst die Akzeptanz von Cloud Computing Jahr für Jahr. Und mit den Modellen SaaS, IaaS, PaaS, SECaaS, SASE und vielen anderen passen sich die Angebote der Cloud-Anbieter an die technischen und rechtlichen Entwicklungen der Unternehmen an. Datensouveränität, Latenzzeiten, Sicherheit der Infrastruktur, Wahl einer öffentlichen, hybriden oder privaten Cloud-Infrastruktur; es stellen sich viele Fragen zur Relevanz dieses Modells. Ein Überblick über die wichtigsten Vor- und Nachteile des Cloud Computing anhand von Expertenmeinungen.

Laut der Oreilly-Studie 2021 „*The cloud in 2021 – Adoption continues*", nutzen heute 90% der Unternehmen das Cloud Computing. Eine besonders starke Annahme in der Softwareindustrie, im Bankwesen, im Einzelhandel oder auch im E-Commerce, die heute jedoch alle zu betreffen scheint.

DIE UNAUFHALTSAME EINFÜHRUNG DER CLOUD

Nach dem „*Computing Cloud Report 2018*" haben fast 86% der befragten Personen Angst vor Sicherheitslücken und Datenverlusten in den Cloud-Umgebungen. Am Tag nach der erzwungenen Einführung der Telearbeit scheinen diese Zahlen in weiter Ferne zu liegen, da die Cloud-Dienste von den Unternehmen offenbar massiv angenommen wurden und so von einer sesshaften Arbeitsweise zu einer hybriden Organisation zwischen Arbeits- und Wohnort übergegangen sind. Microsoft 365, CRM, kollaborative Tools, Videokonferenzen und Remote Office – die hohe Akzeptanz dieser Tools hat es ermöglicht, trotz der Gesundheitskrise Flexibilität und Agilität in die Organisationen zu bringen.

Ist es 2022 noch möglich, eine Organisation ohne die Hilfe von Cloud Computing zu steuern? Das ist schwer vorstellbar, wenn die Nutzer nun einfach von zu Hause aus direkt auf Online-Dienste zugreifen – ohne mehrere Netzwerke und Sicherheitstools zu durchlaufen, wie **Julien Paffumi**, Senior Product Manager bei Stormshield, analysiert: „*Auch wenn die Verwendung eines VPN Telearbeit und Mobilität durch den Zugriff auf Unternehmensressourcen ermöglicht, erfordert es vom Benutzer einen zusätzlichen Aufwand. Im Gegensatz dazu sind Cloud-Plattformen, sei es ein CRM oder eine SaaS-Büroumgebung, direkt von überall und mit jedem Endgerät verfügbar. Diese Zugänglichkeit erleichtert ihre Nutzung und damit ihre Annahme.*" Dank dessen konnten kleine Unternehmen ohne große Datenhistorie ihre Tools schnell auf die Cloud umstellen. Eine Annahme, die durch die aufeinanderfolgenden Lockdowns seit Anfang 2020 erleichtert wurde. SaaS-Anwendungen sind für Administratoren und Benutzer gleichermaßen praktisch, da sie von jedem Ort aus bereitgestellt, konfiguriert und erreicht werden können, ohne dass man sich Gedanken darüber machen muss, welche Software (Server und Clients) bereitgestellt oder welche Fernzugänge geöffnet werden müssen. Ganz zu schweigen von der günstigen Preispolitik, die von Softwareherstellern eingeführt wurde, um Unternehmen zum Umstieg zu bewegen. Für mittlere und große Unternehmen ist die Umstellung jedoch nicht so einfach. Der Wechsel von einer *On-Premise-Lösung* zu einer Cloud-Lösung ist mit Kosten verbunden und muss vorausschauend geplant werden. Migration der historischen Daten, Schulung der Benutzer, Sicherung der Plattform und des Zugriffs – ein Projekt dieser Größenordnung kann sich auf die Produktivität der Mitarbeiter und ganz allgemein auf die Sicherheit des Unternehmens auswirken. Dann wird häufiger die Lösung eines Nebeneinanders von *On-Premise*- und Cloud-Infrastruktur bevorzugt.

Als logische Konsequenz nutzen auch geschlossenere Sektoren wie die Industrie das Cloud Computing. Diese Öffnung erfolgt nach einer genauen Bedarfsanalyse, wie **Vincent Nicaise**, Industrial Partnership and Ecosystem Manager bei Stormshield, erläutert: „*In den letzten fünf Jahren haben wir eine maßvolle und fallweise Einführung des Cloud Computing in der Industrie erlebt. Ursprünglich autonome Industrienetzwerke können heute in bestimmten Fällen Daten zur Analyse in virtuelle Umgebungen zurückführen.*" Und das aus gutem Grund, denn die Datenverarbeitung steht heute im Mittelpunkt der Bedürfnisse und Projekte der Unternehmen in diesem Sektor. Durch

die Rückführung der Daten in einen *Data Lake* können mithilfe algorithmischer Modelle prädiktive und präskriptive Analysen erstellt werden. **Diese Rückführung der Daten in die Cloud hat es den Unternehmen ermöglicht, Krisensituationen zu antizipieren und vorherzusagen.** Dies gilt insbesondere für Produktionsumgebungen (zur Vermeidung von Ausfällen und Versorgungsbedarf sowie zur Optimierung der Prozesskontinuität), für Vertriebsteams (zur Visualisierung der aktuellen und zukünftigen Geschäftsleistung) oder auch für Sicherheitsteams (zur Analyse und Verhinderung von Cyberangriffen). Der Industriesektor stößt jedoch auf eine technische Einschränkung, die der Latenzzeit von Cloud-Infrastrukturen. Diese Analyse wird von **Jocelyn Zindy,** Commercial Director Cybersecurity and Digital Transformation bei Eiffage, geteilt: „*Bei der Verwendung von Steuerungsanwendungen muss die Datenverarbeitung im Millisekundenbereich erfolgen. In diesem Fall weicht das Modell des Cloud Computing eher dem Edge Computing, bei dem sich die Verarbeitungsinfrastruktur lokal so nah wie möglich an der Maschine befindet, um dann später die Daten in der Cloud zu teilen.*" Und die Zahlen aus der Studie des IDC im Januar 2022 deuten in diese Richtung, da die Ausgaben für Edge Computing im Vergleich zum Vorjahr um in einem Jahr um 16% gestiegen sind in Europa.

Trotz der vielen Vorteile, die die Cloud bietet, erfordert ihre Einführung daher eine Anpassung der Unternehmen. Weit entfernt vom Marketing-Image einer Integration mit wenigen Klicks und ohne Einschränkungen **erfordert die Einführung der Cloud eine multidisziplinäre Reife innerhalb der Organisationen**. Aber wie hoch sind die Kosten für eine solche Umstellung? Für welchen Bedarf und welchen Datenumfang? Und vor allem: **Mit welchen Sicherheitsregeln?** Diese vielen Fragen erfordern die Anstrengung der Kommunikation zwischen den Teams aus den Bereichen Produktion, Logistik, Marketing, Handel mit den IT- und Sicherheitsteams. Angesichts der Dominanz der GAFAs auf dem Hosting-Markt und der Umsetzung des *Cloud Act* bleibt die Frage der Sicherheit dieser Daten in Cloud-Umgebungen für Unternehmen ein Anliegen, insbesondere für europäische Organisationen.

CLOUD UND CYBERSICHERHEIT – EINE UNMÖGLICHE EHE?

Aufgrund der Herausforderungen in Bezug auf Cybersicherheit und Datenhoheit **bleibt die sichere Speicherung von Daten in der Cloud ein wichtiges Anliegen für Organisationen**. Denn laut dem Barometer zur Cybersicherheit in Unternehmen (Ausgabe 2022), das von OpinionWay und CESIN durchgeführt wurde, ist die Cloud eine Umgebung, die einen besonderen Schutz erfordert. Die Befragten des Barometers nennen die fehlende Kontrolle über die Zuliefererkette des Hosting-Anbieters (48%) und die Schwierigkeiten bei der Zugangskontrolle durch die Administratoren des Hosting-Anbieters (43%) als die beiden wichtigsten Risikofaktoren bei der Nutzung der Cloud. Darüber hinaus sind immer noch mehr als 8 von 10 befragten CISOs der Meinung, dass

die Sicherung der in der Cloud gespeicherten Daten spezielle Tools erfordert (86%), insbesondere Tools, die die vom Cloud-Provider angebotenen Tools ergänzen (63%).

Aber muss man dann heute noch Angst vor der großen bösen Cloud haben? Die Antwort auf diese Frage kann unterschiedlich ausfallen. Während die Nutzung einer nicht souveränen Cloud in sensiblen Umgebungen (wie denen von Betreibern wesentlicher Dienste und Betreibern lebenswichtiger Dienste) verboten ist, entscheiden mittlere und große Unternehmen in traditionellen Branchen allein darüber, wie sie ihre Daten speichern. Und zwar in zwei Kategorien: solche, die in der Cloud geteilt werden können, und solche, die intern bleiben müssen. Jocelyn Zindy meint: „*Die Cloud wird von großen Unternehmen als Werkzeug genutzt, um Daten zu entflechten. Hier laufen die Daten aus verschiedenen Systemen zusammen, aus Industrie-, Produktions-, Infrastruktur-, Energieleistungs- und Rückverfolgbarkeitssystemen. Diese Umgebung unterliegt dann Budget-, Leistungs- und Sicherheitszwängen.*“ Um diesen Herausforderungen zu begegnen, sind Angebote für Sicherheitsprodukte in der Cloud entstanden. Unter den Akronymen SECaaS (*Security As A Service*), SASE (*Secure Access Service Edge)* oder auch FWaaS (*Firewall As A Service*) bieten diese cloudbasierten Sicherheitslösungen Flexibilität für die Sicherheitsteams. Im Mai 2021 kündigte Gartner einen Anstieg um 41% bei den Ausgaben von Unternehmen für cloudbasierte Cybersicherheitsprodukte an – auch wenn dieser Trend derzeit vor allem in den USA zu beobachten zu sein scheint, während Europa insgesamt vorsichtiger ist.

IST EINE SOUVERÄNE EUROPÄISCHE CLOUD WIRKLICH MÖGLICH?

Eine begründete Vorsicht, denn sobald diese Daten durch die Cloud wandern, stellen sich Fragen der Integrität und Vertraulichkeit. Dies gilt umso mehr, wenn diese den Fragen der Territorialität der Gesetzgebung unterliegen, hauptsächlich der US-amerikanischen und der europäischen. Und seit einigen Jahren besteht **auf dem europäischen Markt ein Bedarf an souveränen Cloud-Betreibern, die nicht der US-Gesetzgebung unterworfen sind**.

Schematisch ausgedrückt kann diese US-Gesetzgebung einen Hosting-Betreiber dazu verpflichten, auf Anfrage in einem geregelten Kontext Zugang zu Kundendaten zu gewähren. Als Gegenmaßnahme und mit dem Ziel der digitalen Souveränität und unter deutsch-französischer Führung starteten 22 Mitglieder im Juni 2020 das Projekt GAIA-X. Das Projekt, das ursprünglich als souveränes europäisches Cloud-Projekt geplant war, wuchs im November desselben Jahres von 22 auf 180 Mitglieder an, darunter paradoxerweise auch Akteure wie Alibaba, Amazon, Microsoft und Google. Die Glaubwürdigkeit des Projekts wird dadurch erschüttert ... Nach dem (krachenden) Ausscheiden von zwei Mitgliedern im Jahr 2021 ist das Projekt immer noch in der Entwicklung, stößt aber auf die „*üblichen bürokratischen Hürden der Europäischen Union*“, wie die folgenden Berichte des Marktforschungsunternehmens Forrester zeigen. Und dieses GAIA-X-Projekt ist nicht das erste seiner Art, denn 2012 waren mit Numergy (eine Gründung von Bull und SFR) und Cloudwatt (initiiert von Orange und Thales)

bereits zwei französische souveräne Cloud-Projekte entstanden. Leider hatten beide Projekte ihren Markt nicht gefunden und konnten zwei Jahre später einen Umsatz von 6 Millionen Euro bzw. 2 Millionen Euro für sich beanspruchen; ein Staubkorn angesichts der Milliardenumsätze der GAFAM.

In Frankreich hat die ANSSI bereits 2014 ein Referenzsystem für Anbieter von IaaS- (*Infrastructure as a Service*), PaaS- (*Platform as a Service*) und SaaS-Angeboten (*Software as a Service*) eingeführt, die den Sicherheitsempfehlungen der Behörde entsprechen, genannt SecNumCloud. Hinter dem Versprechen einer vertrauenswürdigen Cloud verbirgt sich diese Zertifizierung, die es ermöglicht, ein hohes Maß an Strenge in Bezug auf die Cybersicherheit mit dem Angebot eines Anbieters zu verbinden. „*Dieser SecNumCloud-Ansatz ist interessant, weil er es ermöglicht, Cloud-Lösungen mit einem hohen Anspruch zu qualifizieren und so Vertrauen in französische Cloud-Akteure zu schaffen*“, erklärt Julien Paffumi. *Dies ist ein gutes Signal an die Unternehmen. Dank dessen ist es möglich, die Cloud über vertrauenswürdige Anbieter einzuführen.*“ In der Folge dieses Ansatzes hat der Hosting-Dienstleister 3DS OUTSCALE, qualifizierter SecNumCloud-Akteur, einen *Marktplatz* entwickelt, der Lösungen von Drittanbietern fördert, um ein sicheres, vertrauenswürdiges und vollständig in Frankreich entwickeltes Umfeld aufzubauen. Ein echtes Alleinstellungsmerkmal also.

Die Macht der Dinge und die Entwicklungen in der Gesellschaft scheinen also die Frage nach einer unumgänglichen Cloud zu beantworten. Aber es bestehen weiterhin die Zwänge der Leistung, der Kosten, der gesetzlichen Territorialität und vor allem der Datensicherheit, die die Grundlage aller Überlegungen von Unternehmen und Organisationen zu diesem Thema bilden müssen. Die Cloud, ja, aber nicht um jeden Preis.