

Dieser Artikel ist in **Zusammenarbeit mit CRONON** entstanden.**III Cronon**

ILLUSTRATION: STUDIO LH

Sicherheit ist auch eine Frage des Standortes

Ein Plädoyer für die 'Cloud von hier'

Cloud Services aus Deutschland sind im Aufwind. Kriterien wie Datenschutz und Datensicherheit, aber auch der Wunsch nach erreichbaren Ansprechpartnern vor Ort werden immer wichtiger und beflügeln den Trend zu einer souveränen 'Cloud von hier'.

„
Je mehr der Geschäftserfolg und die Existenz eines Unternehmens von verfügbaren und sicheren IT-Systemen abhängt, desto wichtiger wird der Stellenwert der IT-Compliance.“

Amerikanische Konzerne prägen nicht nur unseren Geschmack für Cola und Burger, sondern auch unsere Vorstellung von einer 'echten Cloud'. Die großen Hyperscaler AWS, Microsoft und Google sind zum Synonym für flexible IT-Ressourcen aus dem Internet geworden. Kein Wunder, machen sie es Unternehmen doch leicht, ihre digitalen Innovationen voranzutreiben. Doch wenn es um den zuverlässigen Betrieb von geschäftskritischen Systemen geht, rücken andere Kriterien immer mehr in den Vordergrund.

Unternehmen wünschen sich einen verlässlichen Schutz für ihr intellektuelles Eigentum, sichere Lieferketten und eine vertrauensvolle Zusammenarbeit mit Partnern und Dienstleistern. Hier haben lokale Cloud-Provider die Nase vorn. Sie punkten aber nicht nur beim Datenschutz und der besseren Erreichbarkeit. Sie bieten auch noch andere Vorteile, mit denen sie gerade für viele Unternehmen zu einer echten Alternative werden.

Zukunftsfähiger Datenschutz

Nachdem der Europäische Gerichtshof 2020 das "Privacy Shield"-Datenschutzabkommen für ungültig erklärt hat, gehören die USA nicht mehr zu den "sicheren Drittländern". Selbst wenn die Daten in EU-Rechenzentren gespeichert werden, kann nach einer aktuellen Entscheidung der Vergabekammer Baden-Württemberg eine datenschutzrechtlich unzulässige Übermittlung von Daten vorliegen, wenn der Cloud-Provider seinen

primären Sitz in den USA hat. Es ist völlig offen, wann hierfür eine neue Regelung gefunden wird und wie lange diese dann rechtlich Bestand haben wird. Deshalb sind Unternehmen mit einem lokalen Cloud-Provider beim Datenschutz bis auf Weiteres auf der zuverlässigeren Seite.

Datensouveränität und Rechtssicherheit

Die Standortfrage spielt nicht nur beim Datenschutz eine Rolle. Es geht auch um den Schutz vor extraterritorialen Datenzugriffen. Selbst eine Datenspeicherung im EU-Raum kann solche Zugriffe nicht zwangsläufig verhindern, wie der US CLOUD Act zeigt. Mehr Rechtssicherheit bieten Cloud-Provider, die nicht nur ihre Rechenzentren, sondern auch ihren Firmensitz in Deutschland haben. Nicht zuletzt erleichtert ein allgemeiner Gerichtsstand in Deutschland auch die rechtliche Klärung von Konflikten.

Datenhoheit ist aber nicht nur eine Frage des Standortes. Wenn Unternehmen jederzeit die Kontrolle über ihre Daten behalten wollen, müssen sie auch dafür sorgen, dass sie vor den Zugriffen unberechtigter Dritter geschützt sind. Hier geht es um Themen wie Identitäts- und Zugriffsmanagement sowie Verschlüsselung, aber auch generelle Maßnahmen, mit der die Verfügbarkeit und Sicherheit der Daten gewährleistet werden können.

Compliance-First geht nur mit Security-First

Je mehr der Geschäftserfolg und die Existenz eines Unternehmens von verfügbaren und sicheren IT-Systemen abhängt, desto wichtiger wird der Stellenwert der IT-Compliance. Diese setzt voraus, dass alle relevanten IT-Systeme nach aktuellen Standards vor Sicherheitsverletzungen, Ausfällen und Verlust geschützt sind – auch in der Cloud. Eine 'Compliance-First'-Strategie bedeutet somit immer auch eine 'Security-First'-Strategie.

Je nach Unternehmen und Branche müssen unterschiedliche regulatorische Vorgaben auch auf IT-Ebene umgesetzt werden. Die Verantwortung dafür liegt beim Management des Unternehmens. Daran ändert auch ein Wechsel in die Cloud nichts.

Geteilte Verantwortung in der Cloud

Die Vorstellung, dass in der Cloud die Verantwortung für den Schutz und die Sicherheit der Daten automatisch auf den Cloud-Provider übergeht, hält sich hartnäckig. Deshalb kann man es nicht oft genug betonen: Beim Thema Sicherheit gilt in der Cloud das Prinzip der geteilten Verantwortung. Cloud-Provider sind für die Sicherheit der Infrastrukturen verantwortlich, die sie selbst administrieren und dem Kunden als Service zur Verfügung stellen. Für alles, was der Kunde in der Cloud verwaltet, ist er auch selbst verantwortlich. Je nach Cloud-Service sind das Betriebssysteme, Datenbanken, Anwendungen und Daten, aber auch die Verwaltung der Zugangsberechtigungen und der Security-Systeme.

Unternehmen, die das nicht aus eigener Kraft leisten können, profitieren von einem Cloud-Provider, der nicht nur die Infrastruktur managen kann, sondern auch die benötigten Sicherheitslösungen. Dienstleister, die wie Cronon eine lange Tradition im hochverfügbaren und sicheren Hosten von Unternehmensanwendungen haben, verfügen in der Regel auch über umfangreiches Security Know-how und die passenden Managed Security Services. Vom Patch-Management über Firewall- und VPN-Services bis zum DDoS-Schutz können die meisten Sicherheitsanforderungen abgedeckt und alle Maßnahmen gut aufeinander abgestimmt werden. Darüber hinaus können lokale Cloud-Provider oft flexibler agieren als globale Hyperscaler und schon auf Infrastruktur- und Netzwerkebene individuelle Sicherheitsmaßnahmen umsetzen.

Mehr Vielfalt in einer 'Cloud von hier'

Je mehr Workloads in die Cloud wandern, desto vielfältiger werden auch die Anforderungen. Unterschiedliche Cloud-Plattformen für unterschiedliche Projekte nutzen und trotzdem alle Services bei einem Dienstleister bündeln – auch das geht mit einer "Cloud von hier". Hiesige Cloud-Provider haben meist mehr als nur einen Cloud-Typ im Angebot. Von Public Cloud, über Virtual Private Cloud bis zur Managed Private Cloud ist alles möglich, ebenso hybride Lösungen mit Bare-Metal-Servern sowie Container-Plattformen mit Managed Kubernetes. Wenn sie dann auch noch die Sicherheitsrichtlinien des Unternehmens einheitlich über alle Plattformen hinweg umsetzen und managen können, halten sie den IT-Teams der Kunden den Rücken frei und schaffen Freiräume für neue Projekte.



Link zur Cronon GmbH:
<https://cronon.net/>