Whitepaper

Fragen an Ihren Cloud-Serviceanbieter

Erfahren Sie, wie Ihre Daten in der Cloud geschützt werden

intel Security

Inhaltsverzeichnis

Die Beauftragung eines Cloud-Serviceanbieters (CSP) für Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) oder Software-as-a-Service (SaaS) ist bei der Unternehmens-IT mittlerweile gängige Praxis. Es ist äußerst wichtig, die richtige Wahl in Bezug auf die Anbieter und Dienste zu treffen, vor allem weil es dabei um Sicherheitsprozesse, Datenschutz und operative Fähigkeiten geht. Achten Sie darauf, dass Sie Cloud-Serviceanbieter (CSP) genauestens unter die Lupe nehmen, indem Sie ihnen die richtigen Fragen im Hinblick darauf stellen, wie sie Ihre wichtigsten Daten schützen werden.

Da die Nachfrage nach Cloud-Diensten weiterhin explodiert, bedeutet die Auswahl des richtigen CSP (oder mehrerer Anbieter) eine großen Verantwortung für die Unternehmens-IT und die Sicherheitsexperten. CSPs gibt es in allen möglichen Formen und Größen – von riesigen globalen Unternehmen mit einem breiten Angebot an Cloud-Diensten bis hin zu kleinen Betrieben, die sich auf eine geringe Anzahl an Funktionen spezialisiert haben. Es existieren sogar Cloud-Makler, die Cloud-Dienste von vielen verschiedenen Anbietern mit unterschiedlichen Servicemodellen zusammenführen – von Systemintegratoren und Outsourcing-Unternehmen bis hin zu Software-Anbietern und Fachhändlern.

Dadurch wird es für Unternehmen schwierig, in diesem Labyrinth aus CSP-Optionen die geeigneten Optionen herauszufiltern. Das ist jedoch zwingend erforderlich. Um sich einen Überblick über die vielen Unterschiede zwischen den Anbietern zu verschaffen, müssen Sie ihnen gleichbleibende Fragen zu den wichtigsten Themen stellen. Sicherheit sollte auf Ihrer Liste ganz oben oder zumindest weit oben stehen, wenn Sie sich daran machen, die richtigen CSP-Partner für Ihren Weg in die Cloud auszuwählen.

Wenn Sie Ihre Auswahl weiter eingrenzen, sollten Sie sich mithilfe einer Reihe von Fragen auf die wesentlichen Sicherheitsaspekte konzentrieren. Diese Fragen werden Ihnen dabei helfen, genau zu bestimmen, welche CSPs wirklich alle sicherheitsbezogenen Probleme und Auswirkungen im Blick haben und welche Anbieter einen Ansatz verfolgen, der optimal auf die Prioritäten, Praktiken und die Risikotoleranz Ihres Unternehmens abgestimmt ist. Ein Großteil dieses Whitepapers ist spezifischen Fragen in drei Bereichen gewidmet – Sicherheit, Privatsphäre und Betriebsabläufe – alle in Zusammenhang mit Datenschutz. Wenn Sie diese Empfehlungen beachten und anhand Ihrer eigenen Erfahrungen, eines guten Urteilsvermögens und der Ratschläge von Kollegen, die diesen Prozess bereits durchlaufen haben, eine Wahl treffen, erhöhen Sie damit die Chance, einen oder mehrere CSPs zu finden, die Ihnen dabei helfen, einen zuverlässigen Schutz für Ihre wichtigsten Datenressourcen zu gewährleisten.

Eingehende Prüfung potenzieller CSPs

Ein erster wichtiger Schritt besteht darin, Annahmen bezüglich der Definition von Sicherheit im Hinblick auf einen Anbieter zu vermeiden. Jeder Anbieter ist anders und verfügt über andere Regeln, Service Level Agreements (SLAs) und Geschäftsbedingungen. Sie müssen genau verstehen, zu was sich jeder Serviceanbieter Ihnen, dem Kunden, gegenüber verpflichtet.

Zweitens sollten Sie Fragen dazu stellen, wie mit Datensicherheit und Datenschutz umgegangen wird. Sie müssen wissen, was der Anbieter von Ihrem Unternehmen erwartet, was genau er tut und wie er es tut – und vieles mehr.

Drittens müssen Sie die Geschäftsbedingungen des Anbieters näher betrachten. Natürlich mag sich niemand gern durch die vielen Seiten mit Kleingedrucktem im Vertrag durcharbeiten, doch Sie müssen diese Einzelheiten kennen, um einen Anbieter auswählen zu können, der den richtigen Service bietet und die richtige Vertrauensebene schafft. Also drücken Sie sich nicht vor Ihren Pflichten in diesem Bereich – klicken Sie nicht einfach auf „Bestätigen“ sondern machen weiter. Befassen Sie sich eingehend damit, sehen Sie sich verschiedene Abschnitte innerhalb der Geschäftsbedingungen genauer an, und konzentrieren Sie sich dabei speziell auf die datenbezogenen Aspekte.

Viertens und letztens sollten Sie nicht davon ausgehen, dass alle Cloud-Dienste den gleichen Richtlinien unterliegen und die gleichen Servicebereitstellungsziele haben, nicht einmal bei mehreren Cloud-Diensten desselben Anbieters. Befassen Sie sich mit den Geschäftsbedingungen für jeden einzelnen Dienst. Prüfen Sie sie alle, und treffen Sie keine unbegründeten Annahmen, sonst steht Ihnen am Ende womöglich eine große, kostspielige Überraschung bevor.

Fragen zur Sicherheit

Die gute Nachricht ist, dass die Bedenken hinsichtlich der Cloud-Sicherheit in den letzten Jahren enorm zurückgegangen sind, da CSPs erfolgreich an der Bereitstellung effizienter Sicherheitspraktiken arbeiten. Dennoch zeigen sich viele Führungskräfte sowie zahlreiche Vorstände weiterhin besorgt darüber, ob Unternehmensdaten in der Cloud wirklich sicher sind. Sie sollten Ihren potentiellen CSPs bestimmte Fragen stellen, um ein hohes Maß an Vertrauen aufbauen zu können, das erforderlich ist, um Sorgen und Risiken zu minimieren.

Wer hat Zugang zu meinen Daten, sowohl physisch als auch virtuell?
Physischer Zugang ist etwas komplett anderes als virtueller Zugang. Es ist wichtig, dass Sie Fragen zu beiden Arten des Zugangs stellen.

- Über welche Sicherheitsmaßnahmen verfügt das Unternehmen, wenn auf ihr Rechenzentrum zugegriffen wird?
- Wird dessen Personal einer Sicherheitsprüfung unterzogen und schützt es den physischen Zugang zu den Daten vor Außenstehenden?
- Welche Richtlinien gibt es für den Betrieb oder das Rechenzentrum, und wie werden diese geschützt?
- Wer hat virtuellen Zugang zu den Daten? Von wo aus erfolgt der Zugang und warum?
- Wie erfolgt der Zugang auf die Daten? Nutzen sie VPN und sind die Daten verschlüsselt? Wenn Sie verschlüsselt werden, wie werden die Entschlüsselungsschlüssel gesichert?

Lagert der CSP die Datenspeicherung aus?
Viele Unternehmen nutzen Outsourcing-Unternehmen zur Bereitstellung von Diensten, doch es ist möglich, dass Ihr CSP Ihre Daten an einen anderen Standort oder sogar an einen anderen Anbieter auslagert. Wenn dies der Fall ist, müssen Sie entscheiden, ob Sie dieses Vorgehen für unbedenklich halten.

Wie geht der Anbieter mit rechtlichen Anfragen bezüglich Datenüberprüfungen um?
Unabhängig davon, ob diese Anfragen von ihren Kunden oder von Regierungsstellen stammen und von rechtlichen oder behördlichen Problemen herrühren, erfordert der Umgang mit diesen Anfragen Feingefühl, Erfahrung und Sensibilität gegenüber Unternehmensrichtlinien und Compliance-Vorschriften. Es kann durchaus vorkommen, dass die Qualität Ihrer Daten durch rechtliche Anfragen beeinträchtigt wird, und Sie müssen über die Rückverfolgbarkeit der Daten und die Art des Umgangs mit Anfragen Bescheid wissen.

Wie und wann werden Daten gelöscht?
Da jeder Anbieter anders ist, müssen Sie verstehen, dass es Komplikationen mit der Speicherung geben kann, wenn man bedenkt, wie viele Daten heutzutage die Welt umrunden. Sie sollten sich erkundigen, wie viele Daten von Ihrem CSP gespeichert werden, und vor allem wie viele Ihrer spezifischen Daten gespeichert werden. Zudem sollten Sie fragen, wie lange Ihre Daten gespeichert werden, wann sie gelöscht werden und wie Entscheidungen bezüglich Datenlöschungen getroffen werden.

Welche Datenarchitektur liegt vor?
Fragen Sie konkret nach, wie Ihre Daten von denen anderer Kunden in einer Multi-Tenant-Umgebung isoliert werden. Bitten Sie Ihren Anbieter darum, zu erläutern, wie Ihre Daten von anderen Kundendaten segmentiert werden und wie sich dies in der Zukunft unter Umständen ändern wird.

Welche Zertifizierungen und/oder unabhängige Audits werden durchgeführt?
Zertifizierungen sorgen für ein besseres Verständnis dafür, wie gereift der Anbieter ist, um welche Dinge er sich kümmert und ob er sich kontinuierlicher Verbesserung verschrieben hat. Im Hinblick auf ein unabhängiges Audit empfiehlt sich die Frage, wie häufig der Anbieter sich mit Änderungen befasst und sicherstellt, dass er den Erwartungen seiner Kunden und Lieferanten entspricht.

Fragen zum Datenschutz

Sicherheit und Datenschutz sind eng miteinander verknüpft, es gibt jedoch eine Reihe von Fragen, die sich speziell auf den Datenschutz beziehen und die Sie Ihren CSP fragen sollten. Und Fragen hierzu beschränken sich nicht nur auf gesetzliche Vorschriften, obwohl Datenschutz natürlich in der Einhaltung gesetzlicher Bestimmungen begründet ist.

Welche Daten unseres Unternehmens werden erfasst und wie werden sie geschützt?
Datenschutz gestaltet sich bei jedem Unternehmen ein wenig anders. Demnach ist es vor allem wichtig festzulegen, was Datenschutz für die Interessengruppen innerhalb Ihres Unternehmens bedeutet.

Für was werden die Daten genutzt?
Es ist oftmals ganz erstaunlich, wenn man erfährt, für welche unterschiedlichen Zwecke die eigenen Daten verwendet werden – einige davon werden Sie überraschen oder vielleicht sogar beunruhigen. Achten Sie darauf, dass Ihr CSP Ihre Unternehmensrichtlinien im Hinblick auf die zulässige Nutzung von Daten kennt.

Wie lange werden diese Daten vom CSP aufbewahrt?
In den Geschäftsbedingungen ist möglicherweise angegeben, dass die Daten für eine Dauer von 30 oder vielleicht 90 Tagen oder sogar einem Jahr erfasst werden. Dies schreibt jedoch nicht zwangsläufig vor, wie lange das Unternehmen Ihre Daten tatsächlich aufbewahrt. Dies ist bei jedem Anbieter, bei jedem Dienst und bei den einzelnen erfassten Daten ganz unterschiedlich. Es gibt Daten, die anonymisiert, gespeichert und viele, viele Jahre zu Prüfzwecken verwendet werden. Daher sollten Sie unbedingt Fragen zur Aufbewahrung stellen.

Verschlüsselt der CSP Ihre Daten und auf welche Art und Weise?
Dies sollten Sie unbedingt wissen, um sicherzustellen, dass alle Daten, die Sie als vertraulich bzw. privat einstufen oder um die Sie sich anderweitig Sorgen machen, nicht von dem CSP für andere Zwecke genutzt werden.

Wo werden die Daten gespeichert?
Gibt es bei Ihnen Regeln oder Vorschriften bezüglich der geografischen Datenspeicherung, die die CSPs beachten müssen? Cloud-Serviceanbieter speichern Daten an vielen verschiedenen Orten für viele verschiedene Zwecke, und Sie müssen wissen, ob und inwieweit dies Ihren Geschäftspraktiken entspricht.

Werden Daten zusammengefasst und an andere interne oder externe Stellen weitergeleitet?
Wir alle wissen, dass dies im Internet allgegenwärtig ist und dass es jede Menge Opt-In-/Opt-Out-Programme gibt. Es ist wirklich wichtig, dass Sie erfahren, ob der CSP Daten an andere weitergibt, wie er sie weitergibt, wann er sie weitergibt, warum er sie weitergibt und wo diese übertragen werden.

Fragen zu Betriebsabläufen

Die Aktivitäten Ihrer CSPs überschneiden sich, über die Sicherheit und den Datenschutz hinaus, mit vielen alltäglichen Betriebsabläufen in Ihrem Unternehmen. Wenn Sie dies verstehen, hilft Ihnen das, zu bestimmen, ob die Art und Weise, wie CSPs mit Ihren Daten umgehen und sie an Ihre Partner weitergeben, Ihre Betriebsabläufe unterstützt oder beeinträchtigt.

Welches Redundanzmodell für die Datenbank- und Speicherarchitektur liegt vor?
Gerade Redundanz ist von enormer Bedeutung, da es hierbei insbesondere darum geht, wie man mit Infrastrukturausfällen umgeht, ohne die Geschäftskontinuität zu beeinträchtigen.

Wie häufig werden Backups durchgeführt?
Wir alle haben dieses Mantra im Ohr, seit Computer erstmals auf den Markt kamen: Daten sichern, sichern, sichern. Und es ist äußerst wichtig, die Häufigkeit zu kennen, mit der CSPs Backups durchführen. Je häufiger Backups durchgeführt werden, desto besser ist natürlich Ihre Redundanz. Dadurch kann Ihr Anbieter den Dienst leichter auf einen bestimmten Zeitpunkt zurücksetzen, falls es zu einem Ausfall kommen sollte.

Wie lange dauert die Wiederherstellung nach einem Ausfall?
Ihr Anbieter wird zwangsläufig irgendwann einmal ein Problem haben. Sie müssen unbedingt wissen, wie lange Ihr CSP benötigt, um Ihre Daten wiederherzustellen. Sind es Minuten, Stunden, Tage oder Wochen? Ausfälle treten unweigerlich auf, doch Sie müssen wissen, wie schnell eine Wiederherstellung nach so einem Ausfall erfolgt, wenn Sie einen Serviceanbieter nutzen.

Wie können wir auf Daten aus einem Dienst zugreifen oder diese herunterladen?
Wenn Sie diese Frage stellen, erfahren sie etwas über die unterschiedlichen Philosophien von Serviceanbietern und erhalten einen besseren Einblick darin, inwieweit diese Schritte mit Ihren betrieblichen Prozessen übereinstimmen oder damit im Widerspruch stehen.

Welche Analysetools stehen zur Verfügung, um Ihre Daten zu prüfen?
Der Serviceanbieter verfügt eventuell über eine Vielzahl Ihrer Daten, und Sie möchten wahrscheinlich nicht sämtliche dieser Daten herausziehen und externe Analysetools nutzen, um sie zu komprimieren und Schlussfolgerungen daraus zu ziehen. Es ist sehr viel vorteilhafter, wenn der Serviceanbieter diesen Dienst bereitstellt, sodass Sie eine Aggregation vornehmen und Datenmodelle erstellen können.

Welchen Datenverlust kann man maximal erwarten, wenn Datenkorruption auftritt?
Dies sollte mit den bereits erwähnten Fragen zur Redundanz und Wiederherstellung verknüpft sein, und sie sollten eng aufeinander abgestimmt werden. Wie lange dauert eine Wiederherstellung nach einem Datenverlust und inwieweit wird dieser Wiederherstellungsprozess tatsächlich die Datenqualität beeinträchtigen?

Zusammenfassung

Diese empfohlenen Fragen sollen Sie bei Ihrem Prozess der Ermittlung, Beurteilung und Auswahl von sowie in der Zusammenarbeit mit CSPs unterstützen. Diese Fragen dienen zudem als wichtige Realitätsprüfungen bei Ihrer laufenden Bewertung der Leistung Ihres derzeitigen CSPs und als regelmäßig festgelegter Maßstab für neue Dienste, die Sie beim weiteren Ausbau Ihres Geschäft unter Umständen benötigen.

Denken Sie daran, dass die Auswahl eines CSPs keine triviale Angelegenheit ist. Eine falsche Wahl kann enorme, ja möglicherweise sogar katastrophale Auswirkungen auf Ihr Unternehmen haben, wenn die Sicherheitsleistungen Ihres CSPs nicht Ihren Bedürfnissen entsprechen – jetzt und in Zukunft. Gleichzeitig kann die Auswahl des richtigen CSPs Ihrem Unternehmen in vielerlei Hinsicht von Nutzen sein – in wirtschaftlicher Hinsicht, bei der internen Ressourcenzuweisung, in Bezug auf das Vertrauen in die Sicherheit und Integrität Ihrer Daten und noch bei vielem mehr.

Wenn Sie diesen Prozess der Beurteilung potenzieller CSPs vor sich haben, können diese Fragen bezüglich der Sicherheit, des Datenschutzes und der Betriebsabläufe Ihr Vertrauen in die endgültige Auswahl Ihrer CSP-Partner stärken. Natürlich sollten diese Fragen abgewogen und angepasst werden, um dem Geschäftsmodell, den betrieblichen Prioritäten und der Kultur Ihres Unternehmens Rechnung zu tragen. Die Verwendung dieser Fragen ist aber in jedem Fall eine effektive und effiziente Möglichkeit, um klügere Entscheidungen im Hinblick auf Partnerschaften zu treffen, wenn Sie die Nutzung von Cloud-Diensten ausbauen.

Das mag nach extrem vielen Fragen aussehen, doch glauben Sie uns – auf lange Sicht werden Sie froh darüber sein, die Zeit darauf verwendet zu haben, sie alle durchzugehen. Es ist sehr viel besser, dank dieser Fragen über handfeste Informationen zu verfügen als die Antworten erahnen zu müssen.

Weitere Informationen finden Sie unter **www.mcafee.com/de/solutions/secure-cloud/index.aspx**.

Über den Verfasser

Jamie Tischart
CTO Cloud/SaaS, Intel Security

Jamie Tischart ist als CTO für Cloud/SaaS bei Intel Security tätig und ist in leitender Funktion für die Entwicklung künftiger Cloud-Lösungen von Intel Security sowie für die Schaffung eines nachhaltigen Wettbewerbsvorteils verantwortlich. Er arbeitet seit mehr als 10 Jahren bei Intel Security und hat bereits zahlreiche technische Positionen übernommen, darunter Senior Director of Cloud Engineering, Operations and Research und Senior Director bei McAfee® Labs, Quality Engineering and Operations. Bevor er zu McAfee wechselte, bekleidete Tischart mehrere leitende Positionen in den Bereichen Qualitätssicherung, Management sowie Engineering bei Unternehmen wie MX Logic, Blackbaud, Openwave, Newbridge Networks und Corel. Tischart verfügt über einen MBA-Abschluss von der Aspen University. Er lebt mit seiner Familie in Colorado, wo er seiner Leidenschaft für SaaS-Entwicklung, DevOps und den Cloud-Betrieb sowie Agile Coaching und Quality Engineering Leadership nachgeht, während er zudem in seiner Freizeit gern Ski fährt, schreibt und Hockey spielt. Er setzt sich als Freiwilliger aktiv für viele Organisationen ein, darunter Habitat for Humanity, Ronald McDonald House Charities of Denver, Inc., und Food Bank of the Rockies.

Über Intel Security

Intel Security setzt sich mithilfe seiner McAfee-Produktlinie dafür ein, dass die digitale Welt sicherer und für jeden besser geschützt wird. **www.intelsecurity.com**. Intel Security ist eine Division von Intel.

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com

62487wp_questions-cloud-service-provider_0616