Grundlagen der Cloud-Sicherheit

WHITEPAPER

Inhaltsverzeichnis

Trotz der schnellen Verbreitung von Cloud-Computing gibt es keinen einzigen vorgefertigten Plan dafür, wie Unternehmen Cloud-Modelle implementieren und nutzen. Unternehmen nutzen private und öffentliche Clouds und kombinieren beides oftmals in einer hybriden Cloud. Sie implementieren Modelle für Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) und Platform-as-a-Service (PaaS). Einige IT-Teams stellen geschäftskritische Anwendungen in einer einzigen privaten Cloud bereit, andere wiederum verwenden mehrere Clouds für die gleiche Art von Anwendungen. Einige billigen Schatten-IT-Initiativen, während andere davon abraten.

So vielfältig wie Ihre Cloud-Umgebung auch sein mag, wenn Sie damit beschäftigt sind, Cloud-Dienste in Ihrem Unternehmen zu überwachen oder zu implementieren, gibt es eine unantastbare Regel, an die Sie stets denken müssen: Unabhängig davon, wie einfach oder komplex Ihre Cloud-basierten Implementierungen sind, dürfen Sie es niemals zulassen, dass die Sicherheit Ihrer Daten oder Anwendungen in irgendeiner Weise kompromittiert wird. Wenn es zu einem Sicherheitsverstoß oder Cyber-Angriff kommt, bei dem Ihre Daten gefährdet sind, oder wenn der Gesetzgeber Sie für Verstöße gegen geltende Vorschriften zur Rechenschaft zieht, nützt es Ihnen nicht besonders viel, mit dem Finger auf einen Anbieter einer öffentlichen Cloud zu zeigen. Letztendlich sind Sie für Ihre eigene Sicherheit verantwortlich – auch wenn Ihr Anbieter der öffentlichen Cloud über ein Modell mit „gemeinsamer Verantwortung“ verfügt.

intel Security

TechTarget Custom Media

EIN WHITEPAPER VON TECHTARGET

Was bedeutet dies nun in der heutigen Zeit mit den unterschiedlichsten Cloud-basierten Implementierungen? Wie lässt sich ein permanenter Schutz gewährleisten, wenn Daten und Anwendungen in mehreren Clouds unterwegs sind – in privaten, öffentlichen und hybriden Clouds? Wo hört bei der Nutzung einer öffentlichen Cloud Ihre Verantwortung für Sicherheit auf und wo beginnt die Verantwortung des Anbieters? Können Sie sicherstellen, dass es keine Sicherheitslücken gibt, wenn Anwendungen und Daten die Peripherie Ihres Netzwerks verlassen? Wenn Sie sich neue Technologien für private Clouds zu eigen machen, beispielsweise ein Software-definiertes Rechenzentrum (SDDC), was müssen Sie über zusätzliches Gefährdungspotenzial wissen?

In diesem Whitepaper werden die Sicherheitsherausforderungen bei den verschiedenen Cloud-Modellen besprochen, die Sie unter Umständen implementieren oder in Erwägung ziehen. Wir führen zudem Richtlinien auf, die gewährleisten sollen, dass die Sicherheit nicht kompromittiert wird – egal wie vielfältig oder komplex Ihre Nutzung von Cloud-Modellen ist. Abschließend bieten wir einen kurzen Überblick über einige der kritischen Technologien, die die Grundlage für umfassende Sicherheit im Zeitalter der Cloud bilden.

Sicherheitsherausforderungen bei den verschiedenen Cloud-Modellen

Unabhängig davon, wie einfach oder komplex Ihre Cloud-basierten Implementierungen sind, dürfen Sie es niemals zulassen, dass die Sicherheit Ihrer Daten oder Anwendungen in irgendeiner Weise kompromittiert wird.

Es ist nicht übertrieben, wenn man sagt, dass die Cloud alles ändert – insbesondere dann wenn es um die Sicherheit geht. Cloud-Computing bringt Sicherheitsherausforderungen mit sich, die sich von den Problemen in der Vergangenheit, selbst in der jüngsten Vergangenheit, ziemlich unterscheiden. Für Sicherheitsexperten geht es nicht nur darum, die Peripherie zu schützen, eine DMZ einzurichten oder die neuesten Viren- oder Malware-Schutzprodukte zu nutzen. Es geht darum, über eine umfassende Sicherheitsstrategie zu verfügen, die ein neues Maß an Transparenz, Einblick, Kontrolle und Schutz ermöglicht – vor allem, da Anwendungen und Daten in zunehmend heterogenen Umgebungen zügig unterwegs sind. Nachfolgend sind die wichtigsten Probleme aufgeführt, die sich jeweils aus den verschiedenen Cloud-Modellen ergeben:

Hybride Cloud

Die hybride Cloud ist eine Cloud-Computing-Umgebung, in der eine Mischung aus privaten Cloud-Diensten vor Ort und öffentlichen Cloud-Diensten von Dritten mit einer entsprechenden Orchestrierung zwischen den beiden Plattformen genutzt wird.[1] Unternehmen verwenden in zunehmendem Maße hybride Cloud-Modelle, da sie der IT flexible Bereitstellungsmöglichkeiten bietet. Einige geschäftskritische Anwendungen können weiterhin unter der IT-Kontrolle innerhalb einer privaten Cloud bleiben. Bei anderen Anwendungen bieten sich eher öffentliche Cloud-Modelle an, da hierbei Vorteile wie elastische Skalierbarkeit, Kosteneinsparungen oder Self-Service-Bereitstellung genutzt werden können.

Hybride Clouds bringen sehr spezielle Sicherheitsherausforderungen mit sich, da Daten und Anwendungen sich in verschiedenen Cloud-Umgebungen hin- und herbewegen: von Ihrem Rechenzentrum in öffentliche Clouds und wieder zurück in Ihr Netzwerk. Wenn Ihre Anwendungen und Daten in die Infrastruktur eines Anbieters von öffentlichen Clouds einfließen, laufen Sie Gefahr, den Überblick und die Kontrolle zu verlieren. Dadurch bietet sich für Malware die Möglichkeit, genau an dieser Stelle einzudringen. Die Herausforderung besteht darin, nicht nur die Transparenz bei allen Computing-Ressourcen – vor Ort und in der öffentlichen Cloud – zu erhöhen, sondern auch eine ständige Überwachung, Schutz, Berichterstattung und Abhilfemaßnahmen innerhalb der gesamten hybriden Cloud-Umgebung durchgehend zu gewährleisten.

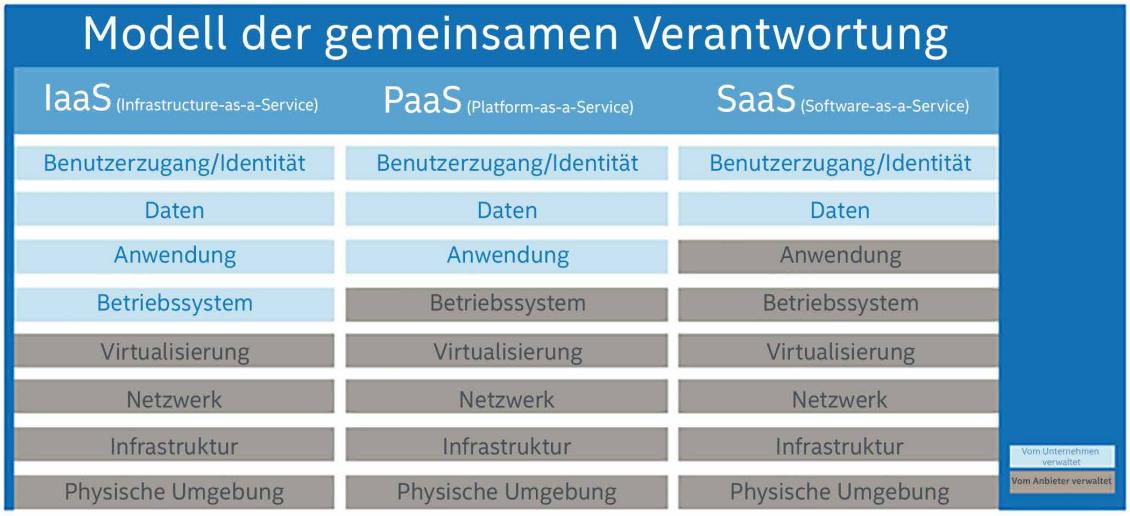
Was Sie beim Einsatz einer hybriden Cloud benötigen, ist eine umfassende Sicherheitsstrategie, die die Transparenz und Kontrolle verstärkt. Sie müssen Sicherheitsmaßnahmen und Richtlinien bei all Ihren virtuellen Maschinen (VMs) auf einfache Weise anwenden können, egal wo sie sich befinden – ob nun in Ihrer privaten Cloud oder innerhalb der Infrastruktur eines Anbieters von öffentlichen Clouds als Bestandteil Ihrer hybriden Cloud-Umgebung.

Öffentliche Cloud

Eine öffentliche Cloud ist eine Cloud-Infrastruktur, die für die Nutzung durch die allgemeine Öffentlichkeit zur Verfügung steht. Sie ist im Besitz eines Unternehmens, einer akademischen oder staatlichen Organisation oder einer Kombination daraus und wird von diesen verwaltet sowie betrieben. Sie befindet sich am Standort des Cloud-Anbieters.[2] Im Hinblick auf die Sicherheit birgt die öffentliche Cloud viele der Gefahren, die wir bereits im Abschnitt zur Hybrid-Cloud besprochen haben. Ihre Daten und Anwendungen entziehen sich zunehmend Ihrem Blickfeld sowie Ihrer Kontrolle und gelangen in die Infrastruktur eines Anbieters von öffentlichen Clouds. Sie müssen wissen, wo Ihre Verantwortung endet und die Verantwortung Ihres Anbieters von öffentlichen Clouds beginnt.

Sie können die Verantwortung für die Sicherheit und Compliance nicht einfach auf die Anbieter von öffentlichen Clouds, in der Annahme, dass sie sich schon darum kümmern werden, abwälzen. Sie müssen das von den einzelnen Cloud-Anbietern bereitgestellte Modell der gemeinsamen Verantwortung für jedes der unterschiedlichen, von Ihnen implementierten Cloud-Modelle – SaaS, PaaS und/oder IaaS – genauestens kennen. Die meisten der großen Anbieter von öffentlichen Clouds, wie beispielsweise Amazon, Google oder Microsoft, beschreiben ihr Modell der gemeinsamen Verantwortung ausführlich auf ihren Webseiten. Nehmen Sie sich die Zeit, um diese Modelle zu verstehen, und wenden Sie diese auf die verschiedenen Arten von Bereitstellungsmodellen an, die Sie unter Umständen nutzen. Und bevor Sie einen Vertrag unterzeichnen, sollten Sie darauf achten, dass die Verantwortlichkeiten einzeln, für jede Art des Dienstes aufgeführt sind.

Ein Beispiel für das Modell der gemeinsamen Verantwortung in Zusammenhang mit einer öffentlichen Cloud ist in der nachstehenden Grafik dargestellt. Hier werden die Systemebenen danach unterschieden, wer für die jeweiligen Punkte verantwortlich ist.



Eines der größten Sicherheitsherausforderungen bei der öffentlichen Cloud ergibt sich dadurch, dass sie so einfach bereitzustellen ist. Der Leiter eines Geschäftsbereichs oder auch ein einzelner Nutzer kann einfach die Webseite eines Anbieters aufrufen und sich mit nur wenigen Klicks und einer Kreditkarte für einen Dienst anmelden. Durch diese Art der Implementierung von Schatten-IT kann das Unternehmen erhöhten Sicherheitsrisiken ausgesetzt werden. Das IT-Team weiß unter Umständen gar nicht darüber Bescheid und der Nutzer ist womöglich nicht mit den verschiedenen Sicherheitskontrollen vertraut, die zum Schutz des Unternehmens erforderlich sind.

Für Sicherheitsexperten geht es nicht nur darum, die Peripherie zu schützen, eine DMZ einzurichten oder die neuesten Viren- oder Malware-Schutzprodukte zu nutzen. Es geht darum, über eine umfassende Sicherheitsstrategie zu verfügen, die ein neues Maß an Transparenz, Einblick, Kontrolle und Schutz ermöglicht.

Eine der zunehmenden Herausforderungen beim Umgang mit der öffentlichen Cloud besteht darin, sich einen Überblick darüber zu verschaffen, wer in Ihrem Unternehmen öffentliche Cloud-Dienste in Anspruch nimmt, welche Art von Diensten sie nutzen – SaaS, PaaS und/oder IaaS – und wie und wann sie diese nutzen. Sobald Sie dies wissen, müssen Sie Technologielösungen nutzen, mit denen Sie ein gewisses Maß an Kontrolle über sie ausüben können, was jeweils von der Art der verwendeten Dienste abhängig ist. In Bezug auf das gemeinsame Sicherheitsmodell ist ersichtlich, dass der Zugang, die Identitätskontrolle und der Datenschutz bei der Cloud-Sicherheit an oberster Stelle stehen sollten – insbesondere bei SaaS-Diensten. Für IaaS-Umgebungen sollten Sie nach einem Sicherheitsprodukt suchen, das eine Dateiintegritätskontrolle und -überwachung ermöglicht, wodurch die Installation nicht autorisierter Software verhindert wird und eine Überwachung jeglicher vorgenommener Änderungen erfolgt. Achten Sie auch darauf, dass Sie eine Lösung nutzen, die einen Host-basierten Überblick über all Ihre Anwendungen bietet.

Private Cloud

Eine private Cloud ist eine Art von Cloud-Computing, das ähnliche Vorteile wie die öffentliche Cloud bietet, einschließlich der Skalierbarkeit und Self-Service-Bereitstellung, jedoch durch eine proprietäre Architektur. Eine private Cloud ist im Gegensatz zu öffentlichen Clouds, die Dienste für mehrere Unternehmen bereitstellen, für ein einzelnes Unternehmen vorgesehen.[3]

Sie können die Verantwortung für die Sicherheit nicht einfach auf die Anbieter von öffentlichen Clouds abwälzen.

Die private Cloud speichert Daten und Anwendungen unter der Kontrolle Ihres Unternehmens, sodass es nicht nötig ist, dass sie außerhalb Ihrer Peripherie in die Infrastruktur eines anderen Anbieters gelangen. Oberflächlich betrachtet scheint es so, dass die Sicherheit viel einfacher zu gewährleisten ist als bei öffentlichen oder hybriden Clouds. In gewisser Weise ist dies auch so, aber wie eingangs erwähnt ändert die Cloud alles.

Private Clouds erfordern neue Bereitstellungsmodelle für Rechenzentren, die die Virtualisierung auf die gesamte Infrastruktur ausdehnen und Unternehmen ermöglichen, Cloud-Funktionen zu nutzen – Ressourcen-Pools, elastische Skalierbarkeit, Self-Service-Funktionen sowie automatische Rückbuchungen. Dadurch kann das Unternehmen von einem mehr am Service orientierten IT-Modell profitieren. Dieses Modell kann jedoch erhöhte Sicherheitsrisiken mit sich bringen, denen vorgegriffen werden muss und die eine entsprechende Planung erfordern.

Ein Beispiel: Da die Virtualisierung innerhalb Ihres Rechenzentrums über Server hinaus auf Netzwerke und Speicher ausgedehnt wird, kommt es zu einem drastischen Anstieg des „Ost-West"-Datenverkehrs zwischen den virtuellen Maschinen (VMs). Ältere Technologien, die sich auf die Peripherie beschränken, haben keinen Einblick in diesen Datenverkehr und sind nicht in der Lage, diesen zu schützen. Sie müssen fähig sein können, Sicherheitskontrollen mit Pakettiefenprüfung für den gesamten Datenverkehr zwischen den VMs anzuwenden.

Ein weiteres Beispiel: Durch die Ausbreitung immer neuer VMs, kann es unter Umständen zu Sicherheitslücken kommen, wenn Richtlinien und Sicherheitsmaßnahmen bei diesen VMs nicht umgehend angewendet werden.

Sicherheitslösungen müssen in die gesamte IT-Umgebung integriert werden und dürfen nicht als Nebensächlichkeit beigefügt werden. IT- und Sicherheitsteams müssen Tools und Technologien verwenden, die speziell für die Bewältigung der Herausforderungen im Zeitalter der Cloud entwickelt wurden.

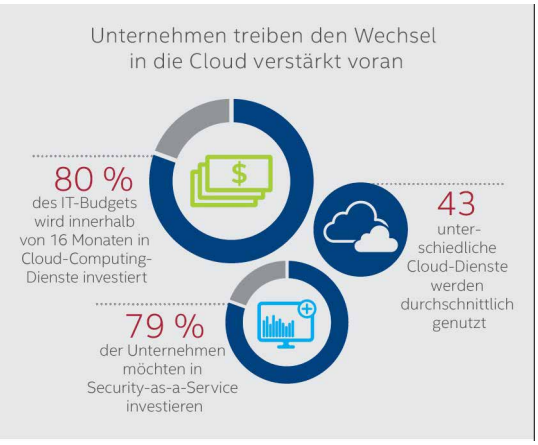
Dies dürfen Sie nicht zulassen. Also müssen Sie in der privaten Cloud versuchen, Sicherheitsmaßnahmen durch ein virtualisiertes oder Software-definiertes Modell anzuwenden, bei dem eine Automatisierung und Orchestrierung von Sicherheitsrichtlinien erfolgt. Dadurch wird der Zeitaufwand und das Risiko in Verbindung mit der manuellen Bereitstellung und Implementierung begrenzt. Wenn die VM verlagert wird, sollten sämtliche Sicherheitseinstellungen und -maßnahmen automatisch mitverlagert werden.

Ein drittes Beispiel: Die Dynamik der Bereitstellung von VMs und die damit verbundene Gesamtlast auf den Servern in einer privaten Cloud-Umgebung kann die Kapazitätsplanung erschweren. Wenn Sie eine Virenschutz-Lösung nutzen, die nicht für virtuelle Umgebungen innerhalb einer privaten Cloud entwickelt wurde, ist dies eine nahezu unmögliche Aufgabe. Selbst wenn herkömmlicher Virenschutz auf diesen VMs ausgeführt wird, ist die Beeinträchtigung der Gesamtleistung innerhalb der Infrastruktur enorm hoch. Das hat direkte Auswirkungen darauf, wie viele VMs auf einem Server laufen können, was sich wiederum auf das vorgesehene Verhältnis zwischen VMs und Server auswirkt – und auch auf die Produktivität. Eine optimierte virtuelle Virenschutz-Lösung ist besser geeignet, um diese elastische Umgebung zu schützen, ohne dabei die Leistung und Skalierbarkeit zu beeinflussen.

Der nächste Schritt

Der Wechsel zu Cloud-Computing ist eine der bedeutendsten IT-Initiativen unserer Zeit. IDC hat dazu gesagt: „‚Cloud First' wird zum neuen Mantra der Unternehmens-IT."[4] Laut eines kürzlich veröffentlichten Berichts von Intel Security zum „Stand der Dinge bei der Migration zur Cloud" werden 80 % der IT-Budgets innerhalb der nächsten 16 Monate für Cloud-Computing-Dienste ausgegeben; 96 % der Unternehmen werden ihre Cloud-Investitionen erhöhen.[5] Zudem verwenden Unternehmen im Durchschnitt 43 verschiedene Cloud-Dienste, 40 % bearbeiten oder speichern bereits sensible Daten in der Cloud. Und während 77 % der Befragten aussagten, dass sie der Cloud jetzt mehr vertrauen als noch vor einem Jahr, haben 66 % auch angegeben, dass die Unternehmensführung ihrer Ansicht nach die Risiken in Verbindung mit der Speicherung von sensible Daten in der Cloud nicht vollständig versteht.

Laut Sicherheitsexperten erfordert die Cloud einen neuen Ansatz. Die Cloud-Sicherheit ist eine ganzheitliche Aufgabe, wobei die Lösungen in die gesamte IT-Umgebung integriert werden müssen und nicht als Nebensächlichkeit beigefügt werden dürfen. IT- und Sicherheitsteams müssen Tools und Technologien verwenden, die speziell für die Bewältigung der Herausforderungen im Zeitalter der Cloud entwickelt wurden. Abschließend müssen diese Tools und Technologien als Bestandteil eines integrierten Bereitstellungsmodells implementiert werden. Sie möchten sicherstellen, dass dieser Schutz fortwährend in sämtlichen Cloud-Umgebungen besteht. Funktionen wie Bedrohungserkennung und Eindringungsschutz müssen in Echtzeit bereitgestellt werden, um das gesamte Unternehmen jederzeit zu schützen, unabhängig davon, wo sich die Daten und Anwendungen befinden.



Bei der Entwicklung Ihrer Sicherheitsstrategie für die Cloud ist es wichtig, mit einem Anbieter zusammenzuarbeiten, der ein integriertes Modell für die Cloud-Sicherheit sowie vielfältige Cloud-spezifische Lösungen bereitstellt. Zu den kritischen Technologien, die Sie unbedingt implementieren sollten, gehören unter anderem ein Software-definierter Sicherheits-Controller, eine virtuelle Netzwerk-Sicherheitsplattform, virtueller Malware-Schutz, Host-basierter Schutz für öffentliche Clouds, fortschrittliche Bedrohungsanalysen und eine zentrale Verwaltung. Diese Lösungen, die miteinander integriert sind, bilden die Grundlage Ihrer Sicherheitsstrategie für die Cloud – jetzt und in Zukunft. Und die Zukunft steht, wie es innerhalb der Unternehmens-IT immer der Fall zu sein scheint, bereits in den Startlöchern.

Wenn Sie für den nächsten Schritt bereit sind, um die Sicherheit Ihrer Cloud-Umgebungen zu gewährleisten, besuchen Sie Intel Security unter: **www.mcafee.com/de/solutions/secure-cloud/index.aspx**.

1 „Hybrid Cloud", SearchCloudComputing, TechTarget

2 „The NIST Definition of Cloud Computing" (Die Definition der US-amerikanischen Standardisierungsstelle NIST für Cloud-Computing), Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, September 2011

3 „Private Cloud", SearchCloudComputing, TechTarget

4 „IDC Predicts the Emergence of 'the DX Economy' in a Critical Period of Widespread Digital Transformation and Massive Scale Up of 3rd Platform Technologies in Every Industry" (IDC prognostiziert die Herausbildung der sogenannten DX-Economy in einer kritischen Zeit der weit verbreiteten digitalen Transformation und der massiven Skalierung von Drittplattform-Technologien in allen Branchen), IDC, 4. Nov. 2015

5 „Blauer Himmel oder dunkle Wolken? Der Stand der Dinge bei der Migration zur Cloud", Intel Security, April 2016

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com