KURZFASSUNG

Das Warum, Was und Wie des Software-definierten Rechenzentrums

Kurzfassung eines Berichts von Osterman Research

Veröffentlicht: Mai 2017

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel.: +1 (206) 683 5683 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

KURZFASSUNG

Bei einem Software-definierten Rechenzentrum (Software-Defined Data Center, SDDC) handelt es sich um einen ganzheitlichen Ansatz für die Einrichtung besserer Rechenzentren. In der grundlegendsten Form ist ein SDDC eine Kombination aus virtuellen Rechnerressourcen und Software-definierten Speicher- sowie Netzwerksystemen, häufig ergänzt um übergreifende Sicherheitsfunktionen.
Mit anderen Worten: Das SDDC fasst nicht nur alle üblicherweise physischen Rechner-, Speicher- sowie Netzwerkaspekte zusammen und automatisiert diese, sondern trägt zusätzlich auch zur Verbesserung der Sicherheit bei.

Durch Nutzung von Virtualisierungsfunktionen kombiniert das SDDC ein Software-definiertes Netzwerk (SDN) mit einem Software-definierten Speicher (SDS). Ein SDDC ist zum Beispiel sinnvoll, wenn Sie ein virtuelles Rechenzentrum (z. B. eine private oder hybride Cloud) einrichten möchten. Viele große Anbieter öffentlicher Clouds nutzen bereits einige Aspekte des SDDC-Ansatzes, um ihre Kosten gering zu halten.

Bei unseren Recherchen stellten wir fest, dass ein Großteil der Server heutzutage bereits in virtuellen Umgebungen ausgeführt wird. Fast die Hälfte der untersuchten Unternehmen plant entweder die Umwandlung ihrer Rechenzentren in SDDCs oder hat diesen Schritt bereits vollzogen. Von den Unternehmen, die eine Umwandlung ihrer Rechenzentren in SDDCs planen, möchte die Mehrheit dies innerhalb der nächsten zwei Jahre in Angriff nehmen.

GRÜNDE FÜR EIN SDDC

Unseren Recherchen zufolge sind die meisten Unternehmen durchaus an einem Wechsel zu einem SDDC interessiert, doch die Mehrzahl dieser Unternehmen sorgt sich auch um die Sicherheit. Als treibende Kräfte für den Wechsel zu einem SDDC wurden neben der Optimierung der Betriebsläufe wurden die Kostensenkung, die geringere Komplexität sowie die Verbesserung der Kontrollmöglichkeiten genannt. Die drei wichtigsten Antriebskräfte sind im folgenden Diagramm dargestellt:

Von Unternehmen genannte Gründe für den Wechsel zu einem SDDC

Quelle: Osterman Research, Inc.

GESCHÄFTLICHE VORTEILE EINES SDDC

Das SDDC bietet eine Reihe wichtiger geschäftlicher Vorteile:

- **Verbesserungen bei der Arbeitsgeschwindigkeit und Produktivität der IT-Mitarbeiter**
  Ein SDDC lässt sich aufgrund seiner äußerst „Software-definierten" Eigenschaften und (mit den richtigen Tools) leichter konfigurieren, umkonfigurieren sowie absichern, wodurch IT-Teams besser auf Änderungen reagieren und effizienter arbeiten können. Darüber hinaus sind in einem SDDC regelmäßige Service-Aktualisierungen möglich und Testumgebungen können schnell eingerichtet bzw. aufgelöst werden.

- **Verbesserungen bei der Sicherheit**
  In einem SDDC können Sie die Kontrolle und Verwaltung der Komponenten des virtuellen Rechenzentrums zentralisieren, wodurch das IT-Team einen besseren

Überblick über diese Komponenten erhält. Zentralisierung sowie Transparenz gehören zu den zentralen Software-definierten Eigenschaften eines SDDC und sind eine wichtige Voraussetzung für einheitliche sowie strenge Sicherheitsmaßnahmen. Während Regeln in von Rechenzentren für mehrere Geräte gelten und von empfindlichen physischen Topologien abhängen, agieren und basieren konsistent umgesetzte Richtlinien in einem SDDC auf logischen, abstrakten Merkmalen der *Workloads* sowie ihrer Daten und nicht auf fragilen, physischen Merkmalen, die über kurz oder lang veraltet sind.

- **Verbesserungen bei der Zuverlässigkeit**
  Traditionelle IT-Abläufe sind grundsätzlich fehleranfällig – selbst wenn Sie eine zentrale Verwaltungskonsole nutzen. Dank der Fähigkeit des SDDC zur Automatisierung von Abläufen werden eintönige, sich ständig wiederholende Arbeiten sowie Fehler reduziert, wodurch wiederum die Sicherheit maximiert und *außerplanmäßige* Ausfallzeiten minimiert werden.

- **Verbesserungen bei der Hardware-Nutzung**
  Virtualisierung führt zu besserer Hardware-Nutzung, sodass Unternehmen ihr Kapital effizienter einsetzen können. So können beispielsweise Software-definierte Rechner- und Speicherressourcen von mehreren Workloads genutzt werden. Zudem vereinheitlicht das SDDC die normalerweise in separaten Einheiten aufgeteilten Netzwerkfunktionen sowie die Funktionen des Speicher-Arrays.

- **Möglichkeit einer interoperablen Cloud**
  Mit einem SDDC können Unternehmen die systeminternen Vorteile hybrider Clouds ganz ohne Anbieter- oder Technologiebindung nutzen. Die Kombination aus Automatisierung, Zusammenfassung, Transparenz und Kontrolle schafft eine Konsistenz, mit der die Verlagerung von Workloads in öffentliche oder private Clouds noch einfacher wird, als dies durch Virtualisierung allein möglich wäre.

MEHR SICHERHEIT DANK SDDC

Beim Thema Sicherheit in SDDC-Umgebungen sollten Sie einige wichtige Dinge im Blick haben:

- Durch den Wechsel zu einem SDDC ändern sich weder die Sicherheitsbedrohungen an sich, noch ist ein anderes Know-how für die Bewertung dieser Bedrohungen und der damit verbundenen Risiken erforderlich. Im SDDC sind Sicherheitsmaßnahmen nicht mehr an einen physischen Punkt im Netzwerk gebunden, da Netzwerk- und Sicherheitsfunktionen nicht mehr an die zugrunde liegende Hardware-Plattform gekoppelt, sondern auf der VM-Plattform (virtuelle Maschine) zusammengefasst sind.

- Als einer der wichtigsten Sicherheitsvorteile überwacht die VM-Plattform des SDDC das Verhalten aller verwalteten Workloads – sowohl innerhalb als auch *zwischen* den virtuellen Maschinen. Dadurch können die VM-Plattform und die Sicherheits-Software das Verhalten *im Kontext* betrachten.

- Die Sicherheits-Software profitiert davon, dass Auswertungen in die Nähe der Workloads stattfinden. Als einer der wichtigsten Vorteile erhält die Software zum Beispiel einen besseren Überblick über gespeicherte und übertragene Daten.

- Durch die Nähe zu den Workloads kann die Sicherheits-Software besseren Schutz vor Denial-of-Service-Angriffen, böswilligen Ausbruchsversuchen aus virtuellen Maschinen, Verstößen gegen Zugangskontrollen an geografischen Standorten und anderen Problemen bieten.

- Das SDDC ermöglicht die Untersuchung potenzieller Bedrohungen auf Basis von Verhaltensinformationen, die in einem herkömmlichen Rechenzentrum selten zur Verfügung stehen. Dadurch ist es einfacher, eine Verbindung zu externen Bedrohungsanalysenetzwerken herzustellen und forensische Echtzeitanalysen potenzieller Bedrohungen in einer virtuellen „Wegwerf"-Umgebung durchzuführen.

FAZIT

Mit einem SDDC können Unternehmen ihre Sicherheitslage erheblich verbessern, die Kosten für IT-Aufgaben, Investitionen und Betriebsabläufe reduzieren, die allgemeine Zuverlässigkeit ihrer Netzwerke und Anwendungen steigern sowie durch die Migration zu öffentlichen, privaten oder hybriden Clouds größere Flexibilität erzielen.