Schutz von Anwendungen in virtualisierten und Cloud-Umgebungen mit VMware AppDefense

Obwohl die weltweiten Ausgaben für IT-Sicherheit kontinuierlich steigen, ist inzwischen eines von vier Unternehmen davon bedroht, Opfer einer Datenpanne zu werden.[1] Auch wenn es mittlerweile Tausende von Sicherheitsprodukten auf dem Markt und die entsprechenden Budgets dafür gibt, sind Daten heute nicht sicherer als früher. Dies stellt CISOs (Chief Information Security Officers), die Anwendungen und Daten in immer dynamischeren, verteilten IT-Umgebungen schützen müssen, vor enorme Herausforderungen. Auch die Einführung moderner, agiler Modelle der Anwendungsentwicklung in immer mehr Organisationen hat das Problem, in einer schnelllebigen Geschäftswelt für Sicherheit zu sorgen, noch verschärft. Sicherheit wird häufig als Hindernis für den Unternehmensfortschritt angesehen.

CISOs und ihre Teams stehen beim Schutz ihrer Daten und Anwendungen vor zwei grundlegenden Herausforderungen:

Unerkannte Bedrohungen und falsche Alarme

Herkömmliche Sicherheitslösungen für Endpunkte lösen zahlreiche falsche Alarme aus, sodass Security Operations-Teams viel Zeit damit verschwenden, nicht existierende Bedrohungen manuell zu untersuchen. Oft erkennen sie echte Bedrohungen überhaupt nicht, was noch schlimmer ist.

Schnelllebige, dynamische Umgebungen

Vorhandene Sicherheitslösungen sind nicht auf die Geschwindigkeit moderner Anwendungsentwicklung und -bereitstellung ausgelegt und können nicht Schritt halten, wenn neue Anwendungen eingeführt und aktualisiert werden.

Transformation der Sicherheit durch Virtualisierung

Mit VMware AppDefense sind Unternehmen in der Lage, beide Herausforderungen zu bewältigen. Bei AppDefense handelt es sich um ein Sicherheitsprodukt für Rechenzentrumsendpunkte, das die Erkennung und Behandlung von Bedrohungen in den Virtualisierungs-Layer integriert, in dem sich Anwendungen und Daten befinden. Durch die Nutzung von VMware vSphere® bietet AppDefense drei wesentliche Vorteile gegenüber herkömmlichen Sicherheitslösungen für Endpunkte:

Genaue Kenntnis des beabsichtigten Zustands von Anwendungen – Überwachung anhand des normalen Verhaltens

AppDefense ist in den vSphere-Hypervisor eingebettet und weiß genau, wie sich Rechenzentrumsendpunkte verhalten sollen. Abweichungen werden daher sofort erkannt. Mit diesem kontextabhängigen Wissen lässt sich zuverlässig bestimmen, welche Änderungen zulässig sind und welche Änderungen eine tatsächliche Bedrohung darstellen.

Automatisierte, präzise Reaktion auf Bedrohungen – die richtige Antwort zur richtigen Zeit

Wenn eine Bedrohung erkannt wird, kann AppDefense vSphere und VMware NSX® zur Orchestrierung der richtigen Reaktion auf die Bedrohung starten. Ein manuelles Eingreifen ist dabei nicht erforderlich. AppDefense kann z.B. automatisch:

- Prozesskommunikation blockieren,
- Snapshots von Endpunkten zur forensischen Analyse erstellen,
- Endpunkte vorübergehend anhalten,
- Endpunkte herunterfahren.

AUF EINEN BLICK

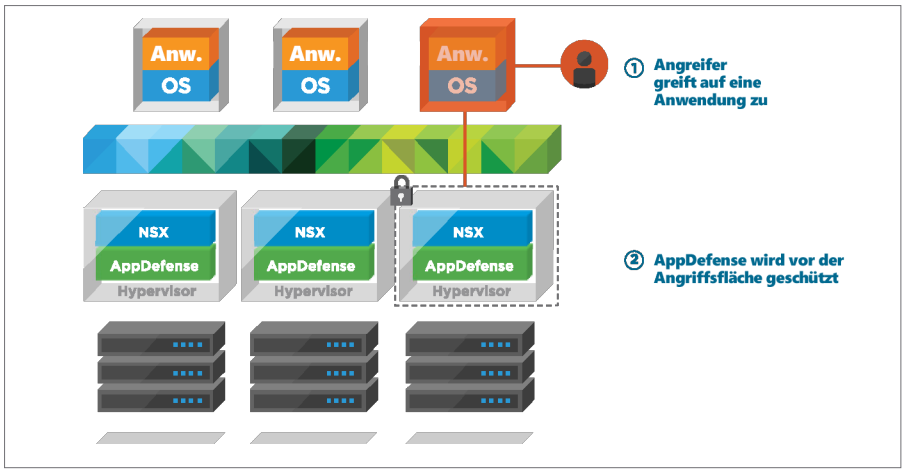
VMware AppDefense™ ist ein Sicherheitsprodukt für Endpunkte im Rechenzentrum, das in virtualisierten Umgebungen ausgeführte Anwendungen schützt. Anders als herkömmliche Sicherheitslösungen für Endpunkte, die Bedrohungen abwehren, überwacht AppDefense Anwendungen auf ihren beabsichtigten Zustand (bzw. ihr gewünschtes Verhalten) hin und reagiert automatisch auf Abweichungen von diesem Zustand, die auf eine Bedrohung hindeuten. Dadurch werden Effizienz sowie Effektivität des Sicherheitsbetriebs maximiert und die Bereitschaftsüberprüfung für Anwendungssicherheit wird optimiert.

DIE WICHTIGSTEN HIGHLIGHTS

- Vereinfachte Sicherheit für Endpunkte im Rechenzentrum
- Verbesserte Erkennung von Bedrohungen im SOC
- Automatische Reaktion auf Sicherheitsvorfälle
- Optimierte Bewertungen der Anwendungssicherheit

Abschottung von der Angriffsfläche – Schutz für den Beschützer

Die erste Aktion der meisten Malware-Varianten beim Erreichen eines Endpunkts besteht darin, die Virenschutzlösung und andere agentenbasierte Sicherheitslösungen für Endpunkte zu deaktivieren. Der Hypervisor bietet einen geschützten Ort, an dem AppDefense ausgeführt werden kann. Selbst wenn ein Endpunkt angegriffen wird, bleibt AppDefense selbst geschützt.



AppDefense in Aktion

AppDefense ist ein grundlegendes Sicherheitsprodukt, das einen weitreichenden Einfluss auf die Sicherheitsstrategie eines Unternehmens hat.

Anwendungsorientierte Warnungen für das Security Operations Center (SOC)

AppDefense erzeugt keine Unmengen von Benachrichtigungen. Wenn es jedoch Alarm schlägt, geschieht das nicht ohne Grund. Die verbindlichen Benachrichtigungen von AppDefense sind mit automatischen Funktionen zur Bekämpfung von erkannten Bedrohungen verknüpft. Sicherheitsadministratoren können also Bedrohungen in der Umgebung aufspüren und beseitigen, ohne große Datenmengen verarbeiten und nicht vorhandenen Bedrohungen nachgehen zu müssen.

Optimierte Bereitschaftsüberprüfung für Anwendungssicherheit

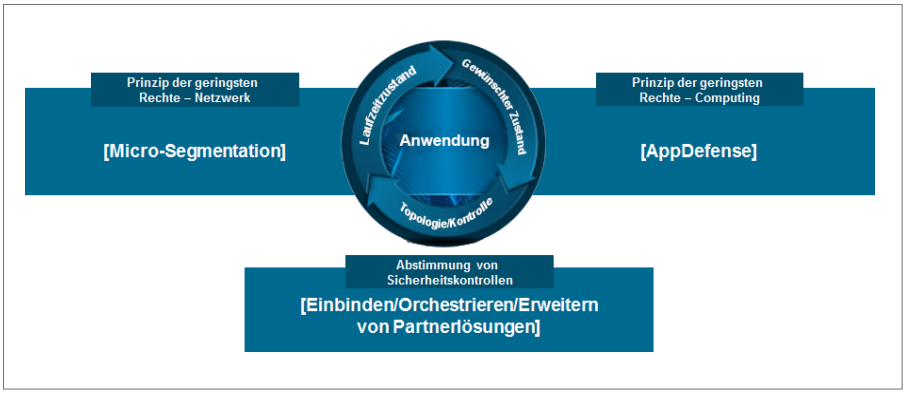
Im Zeitalter der modernen Anwendungsentwicklung werden Anwendungen in kurzen Abständen eingeführt, geändert und wieder eingestellt. Bis ein Sicherheitsteam von der Existenz einer neuen Anwendung erfährt, wurde diese nicht selten bereits geändert. AppDefense schafft eine zuverlässige Informationsquelle zwischen Anwendungs- und Sicherheitsteams und optimiert die Sicherheitsprüfung.

Anwendungsorientierte Sicherheit mit VMware

Mit der Netzwerkvirtualisierungsplattform VMware NSX und ihrer Funktionen für Mikrosegmentierung im gesamten Rechenzentrum hat VMware die Netzwerksicherheit grundlegend verbessert. NSX integriert Netzwerk- und Sicherheitsservices – z.B. Firewalling – direkt in den Hypervisor, wodurch ein Modell basierend auf dem Prinzip der geringsten Rechte für das Netzwerk ermöglicht wird. Damit können Netzwerksicherheitsteams verhindern, dass Bedrohungen sich lateral in ihren Umgebungen ausbreiten.

WEITERE INFORMATIONEN

Wenn Sie VMware AppDefense erwerben möchten oder weitere Informationen benötigen, besuchen Sie unsere Website unter http://www.vmware.com/de/appdefense und testen Sie das Produkt in unserem Hands-on Lab.



AppDefense stellt die Funktionen zur Erkennung und Bekämpfung von Bedrohungen in einem weiteren Kernbereich der Infrastruktur bereit und überträgt das Prinzip der geringsten Rechte so auch auf die Endpunkte im Rechenzentrum. Wird ein Endpunkt angegriffen, erkennt AppDefense die Bedrohung sofort und bekämpft diese automatisch und mit Präzision. Zusammen bieten NSX und AppDefense eine robuste Lösung für den Schutz der Anwendungsinfrastruktur und damit auch der Anwendungen und Daten, die sich darin befinden.

[1] Ponemon Institute, Juni 2017, „2017 Cost of a Data Breach Study: Global Overview“

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Zweigniederlassung Deutschland Willy-Brandt-Platz 2, 81829 München Telefon: +49 89 370 617 000 Fax: +49 89 370 617 333 www.vmware.com/de
Copyright © 2017 – 2018 VMware, Inc. Alle Rechte vorbehalten. Dieses Produkt ist durch US-amerikanisches und internationales Copyright sowie durch Gesetze zur Wahrung des geistigen Eigentums geschützt. Produkte von VMware sind durch ein oder mehrere Patente geschützt, die auf der folgenden Webseite aufgeführt sind: http://www.vmware.com/go/patents. VMware ist eine eingetragene Marke oder Marke von VMware, Inc. oder dessen Tochtergesellschaften in den USA und/oder anderen Ländern. Alle anderen in diesem Dokument verwendeten Bezeichnungen und Namen sind unter Umständen markenrechtlich geschützt. Artikelnr.: vmw53313-sb-securing-app-cloud-env-app-defense-de-DE-a4-101
8/17