5 SCHRITTE ZU UMFASSENDER SICHERHEIT IN SOFTWARE-DEFINED DATA CENTERN

EINFÜHRUNG

Moderne Data Center entwickeln sich schnell weiter. Virtualisierung ebnet den Weg für die Private Cloud und Anwendungen können zu einem Bruchteil der Kosten und Zeit bereitgestellt werden. Virtualisierung löst die Workloads von der Hardware und führt Ressourcen in einem Pool zusammen, sodass diese dynamisch und bei Bedarf zur Verfügung gestellt werden können. Das Ressourcen-Pooling ermöglicht virtualisierte Data Center überhaupt erst und bildet die Grundlage für Private Clouds. Private Clouds sind unternehmensintern implementiert und mit einer Firewall geschützt. Sie werden von der IT-Abteilung administriert und genießen ein hohes Vertrauen, das Public Clouds heute noch nicht entgegengebracht wird.

Private Clouds müssen jedoch nicht zwingend bei einem Unternehmen vor Ort implementiert sein. Dedizierte Cloud-Infrastrukturen können Unternehmen auch exklusiv von einem Cloud-Provider zur Verfügung gestellt werden, der wiederum mehrere Kunden betreut. Dieser Provider – eine dritte Partei oder eine Kombination aus beidem – kann die Cloud-Infrastrukturen besitzen, betreiben und verwalten, wobei diese on- oder off-premise bereitgestellt werden. Unternehmen können zudem hybride Cloud-Architekturen einsetzen, wobei einige der Workloads an eine Public Cloud übertragen werden können.

Unternehmen profitieren bereits seit langem davon, die Kernelemente einer IT-Infrastruktur wie Computing und Storage zu virtualisieren. Dabei blieb eine der wichtigsten Komponenten lange Zeit unbeachtet – das Netzwerk selbst, das zum einen sehr komplex und zum anderen wenig automatisiert ist. Hier vertrauten die Unternehmen auf den manuellen Betrieb, um die Funktionsweise sicherzustellen. Es erfordert eine manuelle Konfiguration, die Switches, Firewalls und anderen Netzwerkkomponenten in das Netzwerk einzubinden. Und so wird das Netzwerk auch zum Flaschenhals für Anwendungen.

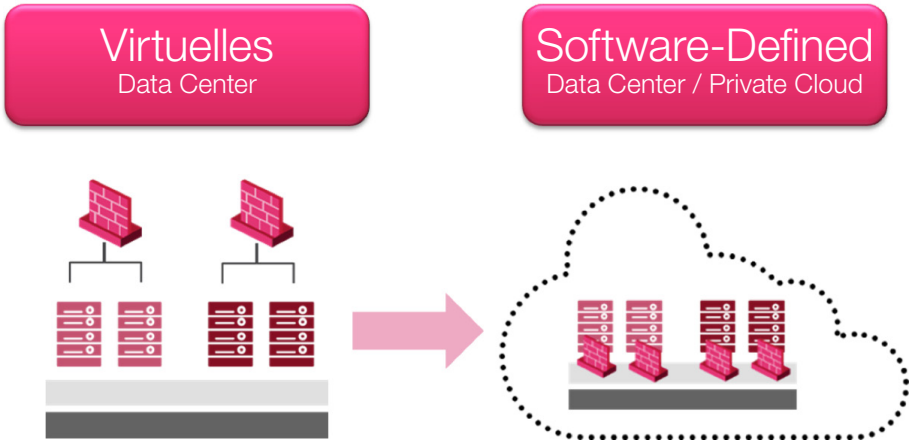

Abbildung 1: Moderne Data Center entwickeln sich aufgrund von Virtualisierungstechnologien rasch weiter.

Jetzt gehen Unternehmen mit ihren Data Centern den nächsten Entwicklungsschritt und virtualisieren auch die Netzwerkebene. Die Netzwerk-Virtualisierung setzt die ganze Leistungsfähigkeit und die Vorteile der Virtualisierung frei und ermöglicht es, Anwendungen zu einen Bruchteil der Kosten und Zeit bereitzustellen.

Dieser Ansatz führte zu Software-Defined Data Centern (SDDC). Hierbei wird die gesamte Infrastruktur – Netzwerk, Storage, Computing und Sicherheit – virtualisiert und als Service bereitgestellt. Die Software automatisiert die gesamte Infrastruktur, stimmt die Services aufeinander ab, integriert alle erforderlichen Sicherheitslösungen und schafft so maximale Flexibilität im Data Center.

SDDCs können heute vollständig mit VMware NSX umgesetzt werden. NSX ist eine umfassende Plattform für die Netzwerk-Virtualisierung, die dank nativer Funktionen wie Isolation, Segmentierung und automatisierten Sicherheitsfunktionen einen verbesserten Schutz bietet. NSX bildet somit die Basis für ein SDDC und ermöglicht eine operativ und wirtschaftlich tragbare Mikro-Segmentierung, die eine automatisierte Bereitstellung, Orchestrierung und horizontale Skalierung der nativen und erweiterten Sicherheitsdienste wie Check Point vSEC umfasst.

Die Integration von vSEC in NSX unterstützt Unternehmen dabei, die Bereitstellung der umfassenden Sicherheitsdienste zu automatisieren und zu vereinfachen. NSX und vSEC stellen gemeinsam eine Lösung für die umfassende Bedrohungsabwehr dar, die in einem Software-Defined Data Center dynamisch bereitgestellt und aufeinander abgestimmt werden kann.

DIE HERAUSFORDERUNGEN IN MODERNEN DATA CENTERN

Die traditionellen Lösungen für Perimeter-Sicherheit können die dynamischen Anforderungen eines modernen Data Centers nicht mehr erfüllen. Zu den Herausforderungen an die Sicherheit, die Unternehme heute bewältigen werden, gehören:

- Die Verlagerung des Datenverkehrs im Data Center – Historisch betrachtet fand ein Großteil des Datenverkehrs zwischen Verbindungspunkten außerhalb der Data Center statt („Nord-Süd“-Verkehr). Dies kam durch die breite Nutzung von isolierten Client-/Server-Anwendungen zustande, die durch die Gateways am Perimeter abgesichert waren.

  Heute hat sich der Datenverkehr der Data Center verändert. Workloads verlagern sich immer stärker in Richtung „Ost-West“ – als Folge der Virtualisierung, der Shared Services und der neuen, verteilten Architekturen von Anwendungen.

  In diesen virtuellen Umgebungen kann die komplexe Kommunikation nur in geringem Maße oder gar nicht von traditionellen Sicherheitslösungen, die üblicherweise für den “Nord-Süd”-Verkehr zuständig sind, überwacht und geschützt werden, da der Datenverkehr das Netzwerk-Perimeter oder das Gateway nicht passiert. Perimeter-Firewalls haben typischerweise nur sehr begrenzte Einblicke in den „Ost-West“-Datenverkehr. Das bedeutet wiederum, dass das Data Center angreifbar und Malware sowie anderen schadhaften Payloads ausgesetzt sein kann.

- Traditionelle Sicherheitsansätze werden oft manuell umgesetzt, lassen sich nur langsam implementieren und sind im Betrieb sehr komplex – Traditionelle Sicherheitslösungen sind nicht darauf ausgerichtet, mit den Veränderungen in dynamischen, virtuellen Netzwerken und der schnellen Bereitstellung von Anwendungen Schritt zu halten. Sich ausschließlich auf Perimeter-Sicherheit zu verlassen, führt zu ressourcenintensiven Engpässen im Netzwerk. Dies wiederum hat erheblichen Einfluss auf die Gesamtleistung des Data Centers, erhöht die Komplexität hinsichtlich der Security und bürdet den Sicherheitsverantwortlichen zusätzliche Last auf.

- Der breite Einsatz von VLANs in Data Centern erhöht das Risiko für alle Anwendungen – Aufgrund der mangelnden Sicherheit zwischen den Systemen (und den VMs) kann eine einzige Sicherheitsverletzung eines virtuellen Hosts es möglich machen, Malware im gesamten Netzwerk zu verbreiten und Anwendungen zu kompromittieren – selbst wenn diese auf verschiedenen VLANs verteilt sind. Erfolgreiche Angriffe auf Dienste mit geringer Priorität können so geschäftskritische Services und sensible Daten Risiken aussetzen, da der Schutz innerhalb der VM („Ost-West“-Datenverkehr) einfach nicht gegeben ist.

Ein Software-Defined Data Center mit einer NSX-Netzwerk-Virtualisierung ermöglicht es Unternehmen, diese Sicherheitsherausforderungen zu adressieren – und zwar flexibel und mit einem hohen Automatisierungsgrad, so wie es für Public- und Private-Cloud-Architekturen charakteristisch ist.

ÜBERBLICK
SICHERHEITSDIENSTE IN SOFTWARE-DEFINED DATA CENTERN (SDDC) AUTOMATISIEREN

Wie bereits erwähnt tragen integrierte Anwendungen, Cloud Computing, zunehmend virtualisierte Data Center und dynamische IT-Umgebungen erheblich dazu bei, dass der Ost-West-Datenverkehr sowie der Datenverkehr innerhalb des Data Centers generell stark zunehmen. Veraltete, hardwarebasierende Ansätze für die Absicherung des Datenverkehrs sind ineffizient und kostenintensiv.

Mikro-Segmentierung mit VMware NSX adressiert die bereits beschriebenen Sicherheitsherausforderungen. NSX Mikro-Segmentierung basiert auf folgenden Grundsätzen:

1. **Automatisierte Integration von Sicherheitsservices in das Netzwerk.** Die Technik der Verkettung von Sicherheitsdiensten ermöglicht es, den Datenverkehr im Data Center automatisiert abzusichern und den Datenverkehr von virtueller Maschine zu virtueller Maschine im Hintergrund zu schützen. Diese Service-Verkettung ist von entscheidender Bedeutung, denn sie ermöglicht Netzwerk-Funktionen wie Sicherheitsservices und Lastausgleich, die bei Bedarf für spezifischen Datenverkehr im Netzwerk oder auch an einer bestimmten Stelle im virtuellen Netzwerk aufgrund vordefinierter Richtlinien und ohne manuelles Eingreifen bereitgestellt werden.
2. **Kontextsensitive Policies.** Um eine Mikro-Segmentierung zu erreichen, müssen die Richtlinien den Status jeder einzelnen Anwendung und ihren operativen Kontext kennen und eine Integration in die Cloud-Orchestrierung und IT-Tools gewährleisten. Hierzu zählen beispielsweise Ticketing-Systeme, Directory-Dienste und SDN-Controller. Die Integration ermöglicht es dem System als Ganzem, die besten Richtlinien – basierend auf dem Zustand und den Zusammenhängen – zu erstellen, zu lernen und anzuwenden. Zudem ermöglicht diese Integration die sichere und skalierbare Bereitstellung der Anwendungen in einem Data Center – und das mit minimalem Aufwand.
3. **Zuverlässige Automatisierung und Orchestrierung.** Um die Automatisierung effizient zu gestalten, müssen die APIs sicher und vertrauenswürdig sein. Sichere APIs ermöglichen die Integration wichtiger Self-Services für Systeme von Drittanbietern, die dann Richtlinien-Änderungen im Rahmen der privilegierten Zugriffsrechte automatisieren können, um das Data Center als Ganzes zu schützen. Das bedeutet, dass Administratoren nur Änderungen von spezifischen Regeln in einer Policy zulassen oder übertragen können.
4. **Erkennung und Analyse von Bedrohungen.** Sobald eine kompromittierte virtuelle Maschine entdeckt wird, sollte diese sofort und automatisch in Quarantäne genommen werden – mit der Möglichkeit, die Probleme zu beheben. Umfassende forensische Berichte und Analysen sind erforderlich, um die Entwicklungen des Datenverkehrs sowie Sicherheitsbedrohungen im Data Center und am Perimeter-Gateway zu erkennen und zu verstehen.
5. **Zentralisiertes Management.** Das Sicherheitsmanagement im Data Center muss einen einheitlichen Einblick in alle virtuellen Umgebungen liefern – dies umfasst virtuelle Maschinen, VMware vSphere vApps™ und Templates in den internen Data Centern sowie in den Private und Public Clouds. So lässt sich eine einzige Sicherheitsarchitektur für das gesamte Unternehmen, alle Systeme und den gesamten Netzwerkverkehr aufsetzen. Diese Management-Lösung sollten flexibel genug sein, um die Sicherheitsdienste von Drittanbietern umfassend in die Netzwerk-Plattform einbinden zu können.

IT-Umgebungen, die moderne Funktionen für die Netzwerksicherheit auf Anwendungsebene benötigen, können VMware NSX nutzen, um Dienste für die Netzwerksicherheit in einer virtualisierten Infrastruktur zu ermöglichen, zu verteilen und durchzusetzen. Umfassende Sicherheitsdienste von Drittanbietern, wie beispielsweise Check Point vSEC, intergieren sich direkt in logische Netzwerke, schaffen Transparenz und sichern den Datenverkehr virtueller Maschinen ab. Zudem überwacht die Software kontinuierlich alle Inhalte und erkennt Bedrohungen unmittelbar.

KERNELEMENTE FÜR UMFASSENDE SICHERHEIT IM SDDC

- **Check Point Appliances und virtuelle Systeme** – Check Point bietet branchenführende Lösungen an, die Leistungsstärke, Multi-Core-Nutzung mit Netzwerk-Technologien kombinieren und somit das höchstmögliche Sicherheitsniveau bieten. Die Security-Gateways sichern den Datenverkehr ab, der in das Netzwerk gelangt oder das Netzwerk verlässt und bieten damit sowohl Schutz am Perimeter und als auch im Kern des Data Center.
- **Check Point vSEC for VMware NSX** – Check Point bietet spezifische, intergierte Lösungen an, die den Ost-West-Datenverkehr in einem Software-Defined Data Center (SDDC) absichern. VMware NSX ermöglicht Mikro-Segmentierung mit einer Vielzahl an virtualisierten Netzwerk-Elementen wie logischen Switches, Routern und Firewalls und bildet so die Grundlage für die Absicherung des Ost-West-Datenverkehrs. Diese Services werden für SDDCs automatisch zur Verfügung gestellt, wenn virtuelle Maschinen bereitgestellt werden. Werden die VMs verschoben, werden diese Dienste ebenfalls automatisch verschoben. NSX bietet darüber hinaus eine Plattform an, um weitere Services, beispielsweise für die Bedrohungserkennung, zu integrieren. So kann Check Point vSEC dynamisch auf der NSX-Plattform bereitgestellt, verteilt und orchestriert werden und die Sicherheit im SDDC automatisieren. Die kombinierte Lösung aus vSEC und NSX bietet den optimalen Schutz vor Bedrohungen und Malware und umfassende Sicherheit für den Ost-West-Datenverkehr.
- **Zentralisiertes Sicherheitsmanagement** – Vereinheitlichtes Management für physische und virtuelle Systeme ermöglicht es der IT-Abteilung, Sicherheitsrichtlinien für beide Umgebungen mit einer einzigen Lösung umzusetzen. Dies garantiert konsistente Sicherheit über alle Gateways hinweg – ohne zusätzliche Investitionen in weitere Management-Konsolen. Dank der Integration in VMware NSX und vCenter und der Nutzung der Richtlinien in NSX- und vCenter können Check Point vSEC und die Check Point Gateway-Appliances sowohl den Ost-West- als auch den Nord-Süd-Datenverkehr umfassend analysieren und schützen.

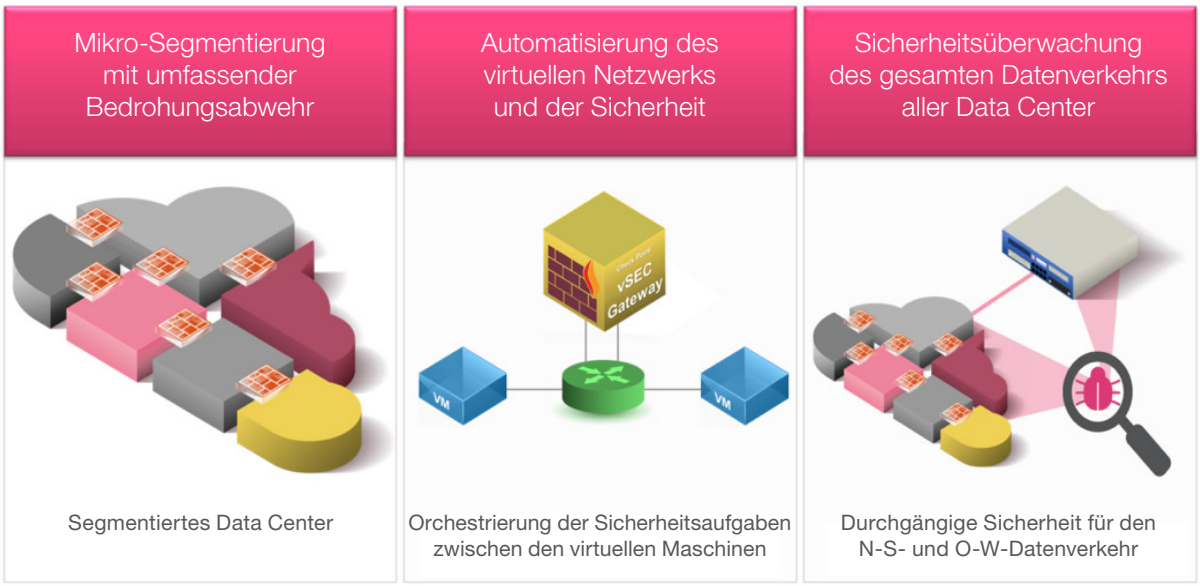

Abbildung 2: Check Point vSEC adressiert alle Sicherheitsanforderungen eines SDDCs

5 SCHRITTE ZU UMFASSENDER SICHERHEIT IN SOFTWARE-DEFINED DATA CENTERN

1. **SICHERER NORD-SÜD-DATENVERKEHR MIT DEN CHECK POINT SECURITY-APPLIANCES:** Wir beginnen damit, den Nord-Süd-Datenverkehr abzusichern, der in das Netzwerk gelangt oder das Netzwerk verlässt. Check Point-Appliances mit Advanced Threat Prevention ermöglichen eine effektive und mehrstufige Verteidigung vor internen wie externen Bedrohungen. Ist beispielsweise eine Anwendung im Data Center infiziert und kommuniziert mit einer Command & Control-Site, wird Check Points Anti-Bot Software Blade dies erkennen und blockieren.

   Check Points Produktlinie der Data Center-Appliances und Data Center-Chassis schützen Hochgeschwindigkeitsnetzwerke mit einem Firewall-Durchsatz von bis zu 1 Tbps, einer sehr geringen Auswirkung auf die Latenz und modularer Skalierbarkeit, sodass die Kapazitäten bei Bedarf erweitert werden können ohne die Leistung oder die Sicherheit zu beschränken.

2. **BEREITSTELLUNG VON CHECK POINT VSEC:** Check Point vSEC umfasst zwei Komponenten: das vSEC-Gateway und den vSEC-Controller. Das vSEC-Gateway ist eine Service-VM (SVM), die auf dem ESX-Hypervisor bereitgestellt wird und vollständig in NSX und vCenter integriert ist. Das Gateway nutzt das VMware NSX-API für die Umleitung und die Prüfung des Datenverkehrs und sichert dabei den Datenverkehr zwischen den VMs über das virtuelle Netzwerk hinweg ab ohne die Netzwerk-Topologie zu verändern. Der NSX-Controller ermöglicht die automatisierte Bereitstellung von vSEC-Gateways auf jedem Host. Die NSX-Plattform für die Service-Integration ermöglicht die Kommunikation zwischen dem vSEC Gateway und dem verteilten, virtuellen NSX-Switch.

   Der vSEC-Controller ermöglicht es dank der Integration in NSX und vCenter, jeden Check Point Security Management-Server in einem SDDC zu nutzen. So kann der vSEC-Controller die Sicherheitsrichtlinien dynamisch anpassen und jedes vSEC-Gateway und jedes physikalische Gateway verwalten, wobei die Administratoren einen umfassenden Einblick in den Datenverkehr des Data Centers erhalten. Die Integration in vCenter und NSX ermöglicht es vSEC, Objekte dynamisch in der Richtlinie von Check Point Security Management anzulegen. Zudem kann der vSEC-Controller jedes Security-Gateway sehr einfach verwalten, auch wenn kein vSEC-Gateway bereitgestellt ist.

3. **SICHERER OST-WEST-DATENVERKEHR MIT CHECK POINT VSEC:** Wie bereits erwähnt ist es für alle Anwendungen von höchster Wichtigkeit, auch den Datenverkehr und alle Geräte innerhalb eines Data Centers abzusichern. NSX und vSEC können den notwendigen Schutz bieten, um das gesamte virtuelle Netzwerk am Perimeter und innerhalb des SDDCs abzusichern. Check Points vSEC-Integration in NSX geht über die Firewall-Funktionalitäten auf Layer 2 bis Layer 4, die VMwares Distributed Firewall (DFW) bietet, hinaus. vSEC bietet zusätzliche Services auf Layer 5 bis Layer 7. Dies umfasst Intrusion Prevention (IPS), Antivirus, Antibot, Anti Spam, Application Control, Identity Awareness und Advanced Threat Prevention.

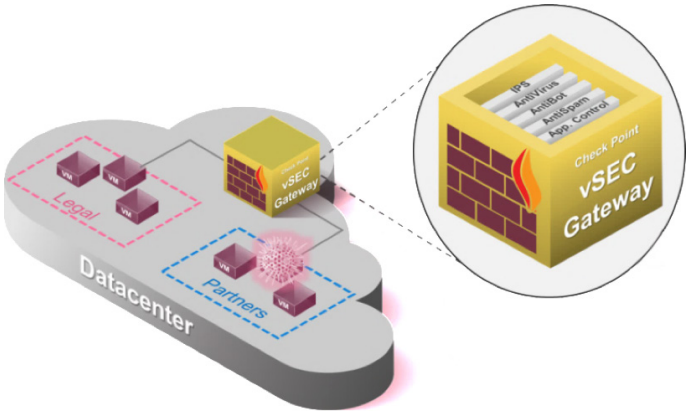

Abbildung 3: Check Point vSEC blockiert die Verbreitung von Bedrohungen innerhalb des Software-Defined Date Centers

   NSX Mikro-Segmentierung ermöglicht es, VM-Ressourcen, auf die spezifische, dynamische Richtlinien angewandt werden, farblich zu kennzeichnen und zu gruppieren und den Datenverkehr auf virtuelle vSEC-Gateways umzuleiten. Diese Gateways nutzen die erweiterte Bedrohungserkennung für den Ost-West-Datenverkehr, um sicherzustellen, dass ein einzelner Sicherheitsverstoß einer Anwendung oder eines Systems nicht die gesamte Infrastruktur nicht kompromittieren kann.

4. **ZENTRALISIERTES MANAGEMENT FÜR SOFTWARE DEFINED DATA CENTER:** Ein voll automatisiertes Software-Defined Data Center nutzt die besten Partner-Services, um die Transparenz zu erhöhen. Dies reicht von individuellen Geräten und Diensten bis hin zu anwendungsbezogenen Richtlinien und detaillierten Einstellungen, die die Verwaltung und die Sicherheit für neue Anwendungen und Workloads automatisieren.

   Check Points Management-Lösung SmartConsole kann sowohl physische als auch virtuelle Gateways verwalten, wie in Abbildung 4 dargestellt. Der vSEC-Controller ist in den NSX Manager und vCenter integriert und kann so die virtuelle Umgebung und den Kontext vollständig erlernen und erfassen. Virtuelle Objekte wie Sicherheitsgruppen oder VMs, die vSEC erlernt hat, können dann in die Sicherheitsrichtlinien, die im Management-Client der SmartConsole definiert werden, aufgenommen und auf den vSEC-Gateways (Service-VMs) eines jeden ESXi-Host installiert werden.

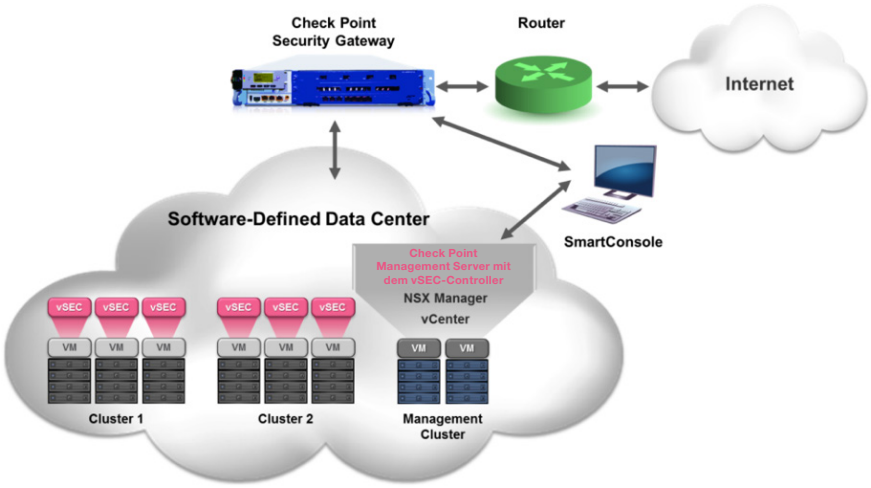

Abbildung 4: Check Point SmartConsole ermöglicht ein durchgängiges Sicherheitsmanagement für SDDCs

NSX-Standard-Tags ermöglichen es, den gesamten Kontext auf den Management-Plattformen VMware NSX, VMware vCenter und Check Point vSEC gemeinsam zu nutzen. Dies stellt sicher, dass die Sicherheitsgruppen und die Identitäten der Virtual Machines (VMs) ganz einfach in die Sicherheitsrichtlinien von Check Point importiert und wieder genutzt werden können. Zudem reduziert dies den Zeitaufwand für die Erstellung von Policies von Minuten auf Sekunden. Check Point vSEC ist unabhängig von der Netzwerk-Topologie und nutzt die vorgegebenen Objekt-Namen basierend auf den Sicherheitsgruppen, den VM-Bezeichnungen, den vCenter-Metadaten und den Metadaten des Data Center-Managements – nicht den IP-Adressen. Dies vereinfacht es, die Policies zu verwalten, die weniger abstrakten Benennungen zu nutzen und eine höhere Transparenz zu schaffen.

Die Kontextsensitivität der Sicherheitsgruppen und VMs wird dauerhaft beibehalten, sodass jegliche Änderung und jegliches Hinzufügen von beispielsweise IP-Adressen, VM-Lokationen oder NSX-Gruppenmitgliedern automatisch in vSec übernommen werden. So können Sicherheitsmaßnahmen auch für virtuelle Anwendungen durchgesetzt werden – ganz gleich, wo diese erstellt werden oder umgesetzt werden sollen. Dies ermöglicht es auch, Richtlinien für Geschäftsbereiche oder für Anwendungen mit Nord-Süd- sowie auch Ost-West-Datenverkehr umzusetzen – über physische und virtuelle Gateways hinweg. Diese Konsolidierung ermöglicht eine einfachere Administration, verständlichere Benachrichtigungen und Berichte. Zudem können IT-Verantwortliche vordefinierte Vorlagen für Check Point-Sicherheitsrichtlinien nutzen und so die Sicherheit von virtuellen Anwendungen erhöhen. Weitere Informationen finden Sie nachfolgend.

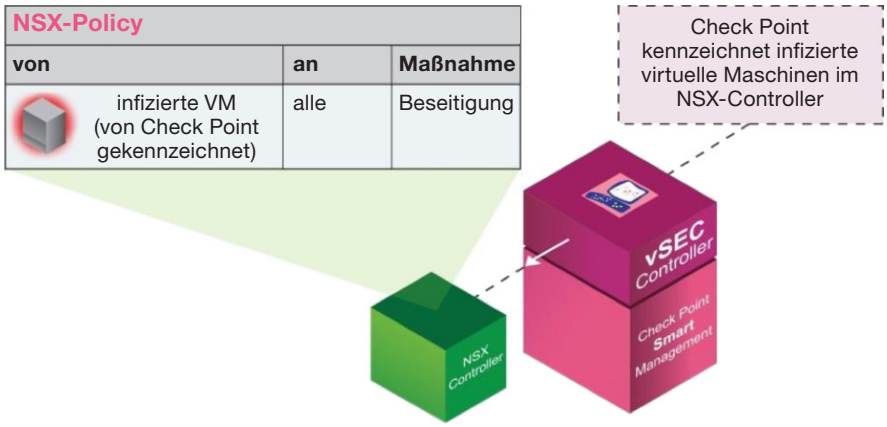

Abbildung 5: Informationen, die zwischen vSEC und NSX ausgetauscht werden, ermöglichen es, Workflows für die automatische Beseitigung von Bedrohungen auszulösen.

Effektives Monitoring und die Analyse von Ereignissen erfordern ein stabiles Sicherheitsmanagement. Unternehmen erwarten Transparenz und Überwachungslösungen, um „das große Ganze“ erkennen und alle relevanten Ereignisse einsehen zu können – ohne eine Vielzahl an Screens, Tools oder anderen Informationsquellen manuell in einen Zusammenhang stellen zu müssen.

Check Points durchdachte Management-Lösungen zentralisieren und vereinfachen das Sicherheitsmanagement für SDDCs erheblich. Check Points SmartDashboard verfolgt und protokolliert alle Bedrohungen über das gesamte Unternehmensnetzwerk hinweg während SmartEvent alle Ereignisse im Data Center visualisiert und in einen Zusammenhang stellt. Check Point stellt hierfür eine zentrale Benutzeroberfläche zur Verfügung.

5. **SICHERE ORCHESTRIERUNG UND AUTOMATION:** Check Points native Integration von vSEC in NSX bietet zahlreiche zusätzliche Sicherheitsfunktionen und verknüpft das Beste aus beiden Welten – erweiterten Schutz, der dynamisch zur Verfügung gestellt wird, und ein enges Zusammenspiel dieser Funktionen in einem hochautomatisierten Software-Defined Data Center.

   Check Point vSEC kann die nativen Sicherheitsfunktionen, die Automatisierung und das flexibel erweiterbare Framework von NSX nutzen, um umfassende Sicherheitsservices in einem SDDC bereitzustellen und miteinander in Einklang zu bringen. Die Netzwerk-Isolation und -Segmentierung der NSX-Plattform ermöglicht eine Mikro-Segmentierung, da die Netzwerkdienste in der Software reproduzierbar sind. Dies schafft so eine grundlegende und sehr umfassende Sicherheit in einem SDDC. Richtlinien werden an den virtuellen Interfaces durchgesetzt und schließen damit auch die Workloads ein. Der Aufwand für eine Rekonfiguration reduziert sich damit von Tagen oder Stunden auf nahezu Null.

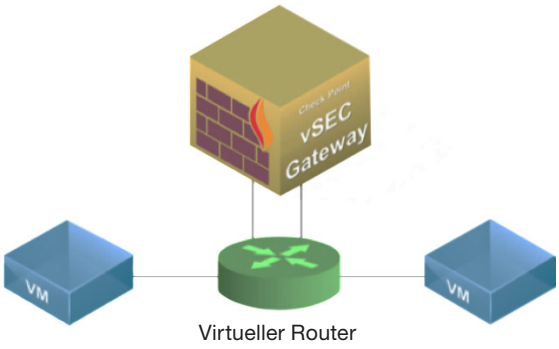

Abbildung 6: Die Sicherheitsfunktionalitäten von vSEC können automatisch zwischen den virtuellen Maschinen aufeinander abgestimmt und bereitgestellt werden.

ERWEITERTE SICHERHEIT DANK MIKRO-SEGMENTIERUNG UND UNTERGEORDENETER RICHTLINIEN

Mikro-Segmentierung bietet grundsätzlich eine höhere Sicherheit für ein SDDC, da diese virtuelle Netzwerke segmentieren und isolieren kann. Untergeordnete Richtlinien in einer Mikro-Segmentierung erhöhen die Sicherheit im gesamten virtuellen Netzwerk zusätzlich und ermöglichen es Unternehmen, dedizierte Richtlinien pro Miko-Segment sowie spezifische, privilegierte Zugriffsrechte für Administratoren zu erstellen.

Untergeordnete Richtlinien in der Mikro-Segmentierung ermöglichen es, Sicherheitsrichtlinien zu erstellen, die alle Aufgaben klar abgrenzen und sehr einfach automatisieren können. Diese einzigartige und leistungsstarke Möglichkeit erlaubt eine sehr granulare Umsetzung von Maßnahmen, wenn Bedrohungen auftreten. Somit ist eine sehr umfassende Überwachung und effektive Sicherheit in Echtzeit in hochautomatisierten Umgebungen möglich.

Der hohe Automatisierungsgrad und die Vereinfachung wirkt sich nicht nur auf die Erstellung von Services in einem Software-Defined Data Center aus, sondern auch auf die Wartung, die Erweiterung oder die Einstellung von Services. Da alle Elemente über virtuelle Devices oder integrierte Sicherheitsrichtlinien gesteuert werden, ist der Verwaltungsaufwand minimal, da „physische“ Änderungen der Richtline sehr schnell und sehr effektiv umgesetzt werden können – ohne die physische Hardware „angreifen“ zu müssen.

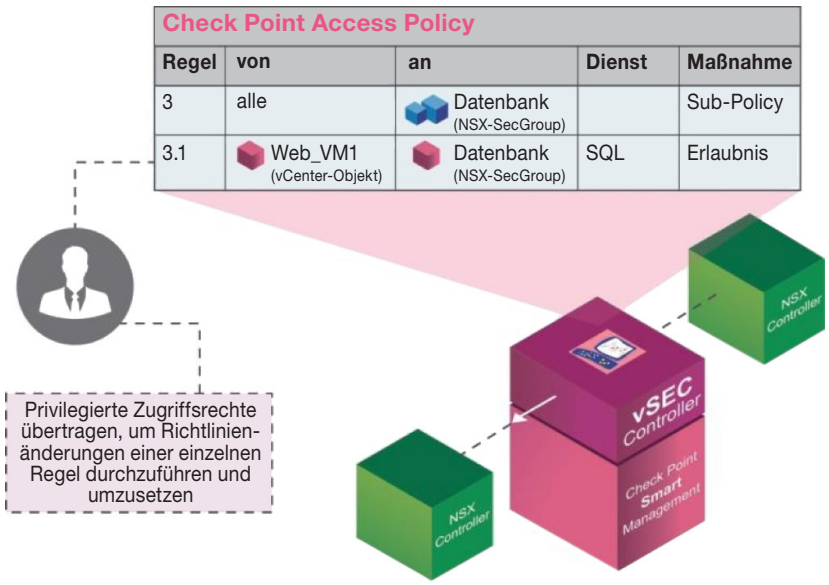

Abbildung 7: Untergeordnete Sicherheitsrichtlinien sind automatisch an NSX-Sicherheitsgruppen und vCenter-Objekte gebunden

ZUSAMMENFASSUNG

Ein Software-Defined Data Center (SDDC) mit der Netzwerk-Virtualisierung VMware NSX ist flexibler, effizienter und sicherer. VMware und Check Point haben in Zusammenarbeit die beste Virtualisierungslösung und die modernsten Technologien für die Bedrohungsabwehr intergiert, um eine effiziente und garantiert sichere Bereitstellung von Anwendungen zu gewährleisten und die Möglichkeiten der Architektur eines Sofware-Defined Data Center in vollem Umfang auszuschöpfen.

Die Kombination von vSEC und NSX lässt die Bedrohungsabwehr tief in die Struktur des Data Center eingreifen. Dies erweitert die Möglichkeiten der nativen Mikro-Segmentierung von NSX und bietet zusätzliche Sicherheitsdienste – wo immer diese auch benötigt werden. Im Falle eines Sicherheitsverstoßes eines Knotens oder eines Netzwerksegments kann die Bedrohung sehr einfach und effektiv in einen Container genommen und damit isoliert werden. Die verteilte Sicherheitsarchitektur ermöglicht es Check Point, die besten Dienste für Netzwerksicherheit auf vNIC-Ebene zu integrieren – für eine äußerst granulare Kontrolle, maximale Transparenz und eine optimale Bedrohungsabwehr.