KURZDARSTELLUNG: 4 HINDERNISSE FÜR DIE PUBLIC-/PRIVATE-CLOUD-SICHERHEIT

Sicherheitsbedrohungen für moderne virtuelle Umgebungen

Zusammenfassung

Durch Virtualisierung und die Cloud können Unternehmen nicht nur Kosten einsparen, sondern auch ihre Effizienz und Agilität steigern. Allerdings müssen sie dazu die ständig wachsende Flut an Malware in den Griff bekommen. Der IT stehen oft nur beschränkte Budgets zur Verfügung, um Public-/Private-Cloud-Umgebungen vor häufigen Problemen und Missständen zu schützen. Dazu gehören unter anderem:

- uneinsehbarer VM-to-VM-Datenverkehr
- unkontrollierte Zunahme von Richtlinien
- Virtual Sprawl
- Public-Cloud-Einschränkungen

Virtualisierung als Erfolgsfaktor

Angesichts schnelllebiger Märkte, eines scharfen Wettbewerbs und einer zunehmend dynamischen Geschäftsumgebung müssen Organisationen nicht nur ihre Marktanteile schützen, sondern auch stetiges Wachstum sicherstellen. Mehr denn je spielen Informationstechnologien hierbei eine zentrale Rolle.

Im Back-End-Bereich wird von der IT erwartet, dass sie mit den neuesten Innovationen Schritt hält, Rechenzentren und die IT-Umgebung modernisiert und IT-Services optimiert, um die Organisation bestmöglich zu positionieren. Dazu gehören die Entwicklung, Implementierung und Nutzung neuer nützlicher Unternehmensanwendungen, Produktivitätstools und -services für Nutzer und Netzwerkarchitekturen wie Private-/Public-/Hybrid-Cloud-Computing, Network-Function-Virtualization (NFV) und Mobility. Gleichzeitig soll die IT auf Basis eines pauschalen – oft knapp bemessenen – Budgets diese dynamische Netzwerkumgebung und die mobilen Mitarbeiter unterstützen und schützen.

Im Front-End-Bereich muss die IT sicherstellen, dass sämtliche webbasierten Interaktionen, Services und Supportleistungen des Unternehmens das ganze Jahr über rund um die Uhr verfügbar sind. Unter anderem muss die IT dafür sorgen, dass sämtliche Websites geschützt sind, ohne Unterbrechung zur Verfügung stehen und einwandfrei funktionieren. Ideal ist ein erschwingliches, aber kompromissloses Sicherheitskonzept. Dafür sind dynamische Sicherheitsfunktionen erforderlich, die Angriffe verhindern und gleichzeitig die nötigen Analysen ermöglichen, um angemessen auf Ereignisse zu reagieren und die physische und virtuelle Infrastruktur der gesamten Organisation zu schützen. Die IT muss auf eine kompromisslose Sicherheit in allen Be-

reichen pochen, sei es in kabelgebundenen/drahtlosen Umgebungen, in der Private/Public Cloud, an zentralen Standorten oder in den IT-Umgebungen von Außenstellen, Zweigniederlassungen, Tochterunternehmen oder Partnern.

Vor- und Nachteile der Virtualisierung

Durch die Servervirtualisierung ist die IT-Welt in den letzten zehn Jahren immaterieller und flüchtiger geworden. Noch heute spielt die Virtualisierung eine wichtige Rolle, da sie nach wie vor bedeutende operative und wirtschaftliche Vorteile für Rechenzentren bietet, Betriebsausgaben und Investitionskosten senkt und es Mitarbeitern erlaubt, sich auf kritische Infrastrukturen zu konzentrieren.

Da Virtualisierungstools und -services immer besser werden – wie zum Beispiel Network-Function-Virtualization – können IT-Abteilungen schnell und einfach virtualisierte Workloads entwickeln und überall innerhalb des virtuellen Netzwerks (VN) platzieren. Die Virtualisierung optimiert zudem Selbstverwaltungsfunktionen und Netzwerkprogrammierbarkeit und sorgt für die nötige Provisioning-Geschwindigkeit, um das Rechenzentrum effizienter betreiben zu können. Auf diese Weise können Netzwerk- und Anwendungsteams neue maßgeschneiderte, auf virtuellen Maschinen gehostete Services entwickeln und bereitstellen und diese jederzeit unmittelbar initiieren, verschieben, kopieren, klonen, wiederherstellen oder löschen, um ihre individuellen Datencenteranforderungen zu erfüllen. Dadurch steigen Agilität und Flexibilität, was eine wesentlich günstigere Bereitstellung von Anwendungsservices im gesamten Unternehmen ermöglicht.

Doch trotz all dieser Vorteile muss sich die IT auch mit den vielen Sicherheitsherausforderungen heutiger Virtualisierungstechnologien beschäftigen (s. Tabelle 2 unten). Durch die Virtualisierung werden automatisch viele Infrastrukturebenen hinzugefügt und die operative Komplexität erhöht. Zum Beispiel begünstigt die gemeinsame Nutzung von Speichern, Routern, Netzwerksegmenten und Kommunikationskanälen erwiesenermaßen Cyberangriffe (z. B. Angriffe, die auf den Missbrauch gemeinsam genutzter Ressourcen basieren oder mehrere virtuelle Maschinen nutzen, sowie Side-Channel-Angriffe oder solche, die häufige netzwerkbasierte Anwendungs- und Protokollschwachstellen nutzen). Diese Bedrohungen betreffen alle Teile des virtuellen Frameworks, einschließlich Hypervisor bzw. Virtual-Machine-Monitor (VMM), virtuelle Maschinen (VMs), Betriebssysteme (OS) in VMs, Anwendungen auf diesen Betriebssystemen sowie die virtuellen Networking-Komponenten der virtualisierten Umgebung. Wird die virtuelle Umgebung unzureichend geschützt, kann dies zu einem beträchtlichen Schaden für die Organisation führen.

Tabelle 2: Zusammenhänge zwischen Schwachstellen und Bedrohungen in Virtualisierungsumgebungen

Bedrohungskategorien		Schwachstellen	Bedrohungen
Offenlegung	Datenlecks	Unzureichender Schutz der ARP-Tabelle	ARP-Table-Poisoning
		Platzierung von Firewall-Regeln innerhalb virtueller Nodes	Umgehung von Firewall-Regeln
	Abfangen von Informationen	Unzureichender Schutz der ARP-Tabelle	ARP-Table-Poisoning
		Übertragung von Daten in vorhersehbaren Mustern	Verkehrsanalyseangriffe
		Unkontrollierte Bearbeitung mehrerer aufeinanderfolgender Anfragen des virtuellen Netzwerks von einer einzigen Einheit aus	Inferenzangriffe und Offenlegung sensibler topologischer Informationen
		Ungeschützter Austausch von Routing-Informationen zwischen virtuellen Routern	Offenlegung sensibler Routing-Informationen
	Ausnutzung der Virtual-Machine-Introspection	Unkontrollierte Virtual-Machine-Introspection	Datendiebstahl
Täuschung	Identitätsbetrug	Ungeeignete Verwaltung von Identitäten:	
		- innerhalb einzelner Netzwerke	Einschleusen bösartiger Nachrichten mit gefälschten Quellen
		- zwischen föderierten Netzwerken	Privilege-Escalation (Rechteausweitung)
		- während Migrationsprozessen	Entfernung von Nodes und erneutes Hinzufügen, um neue (saubere) Identitäten zu erzielen
	Verlust von Registry-Einträgen	Unkontrollierte Rollback-Vorgänge	Verlust von Registry-Einträgen
	Replay-Angriffe	Fehlende eindeutige Message-Identifier	Replay-Angriffe
Störung	Überlastung physischer Ressourcen	Unkontrollierte Ressourcenverteilung	Leistungseinbußen
			Missbrauch von Ressourcen
		Unkontrollierte Bearbeitung von Anfragen des virtuellen Netzwerks	Erschöpfung der Ressourcen in bestimmten Teilen der Infrastruktur
		Fehlende proaktive oder reaktive Recovery-Strategien	Denial-of-Service-Angriffe
	Ausfall physischer Ressourcen	Fehlende proaktive oder reaktive Recovery-Strategien	Ausfall virtueller Router/Netzwerke
		Unkontrollierte Umverteilung von Ressourcen nach Ausfällen	Überlastung der restlichen virtuellen Router nach Ausfällen
Usurpation	Identitätsbetrug	Ungeeigneter Umgang mit Identitäten und den dazugehörigen Berechtigungen	Privilege-Escalation (Rechteausweitung)
	Ausnutzung von Softwareschwachstellen	Privilege-Escalation bei Virtual-Machine-Monitors	Unautorisierte Kontrolle physischer Router

Quelle: „Virtual network security: threats, countermeasures, and challenges“ (Sicherheit virtueller Netzwerke: Bedrohungen, Abwehrmaßnahmen und Herausforderungen), Journal of Internet Services and Applications, Dez. 2015

Mögliche Folgen sind:

- Übernahme virtueller Systeme zur Ausführung bösartiger Aktivitäten
- unerlaubter Zugriff auf geschützte Datenressourcen
- Informationsdiebstahl
- Serviceunterbrechung oder Beeinträchtigung des ganzen virtuellen Ökosystems bzw. von Teilen davon

Das Thema Schwachstellen und Bedrohungen in virtualisierten Systemen stößt derzeit auf großes Interesse – sei es im akademischen Bereich, im Rahmen von Bug-Bounty-Programmen, im Ethical Hacking und in der organisierten Cyberkriminalität. Neue Bedrohungen werden regelmäßig entdeckt. VENOM, CVE-2015-3456, ist etwa ein Exploit, der gängige Virtualisierungsplattformen wie Xen und KVM betrifft.

Die IT hat also allen Grund, sich Gedanken über ihre aktuelle Sicherheitsstrategie zu machen. Viele Organisationen befürchten, dass ihre bestehenden Sicherheitssysteme nicht über die nötigen dynamischen Sicherheitskontrollen und -funktionen verfügen, um virtuelle Infrastrukturen kontinuierlich und angemessen zu schützen. Für die IT ist es daher zunehmend schwierig, einen unterbrechungsfreien Betrieb, die Bereitstellung von Services, eine hohe Verfügbarkeit sowie die Einhaltung gesetzlicher Anforderungen sicherzustellen.

Szenario aus der Praxis

Um das Ganze zu veranschaulichen, sehen wir uns ein Szenario an, bei dem die virtuelle Umgebung einer Organisation in einer physischen Firewall-Sicherheitsarchitektur vorliegt. Abbildung 1 (oben rechts) stellt den Kommunikationsfluss von der Anwendungs-VM zur Datenbank-VM auf der virtuellen Host-Maschine dar. Bei der Anwendung könnte es sich um Microsoft SharePoint bei der Ausführung eines Schreib-/Lesevorgangs in einer SQL-Datenbank handeln. Hier muss die IT für eine sichere Bereitstellung der Anwendungsservices sorgen.

Virtuelle Umgebung mit physischer Firewall

Bei älteren Methoden stehen der IT zwei Prüfansätze zur Verfügung. Eine Möglichkeit wäre, den VM-to-VM-Datenverkehr über einen virtuellen Switch (vSwitch) nach Norden zur externen Switching-Fabric zu routen und ihn anschließend zu

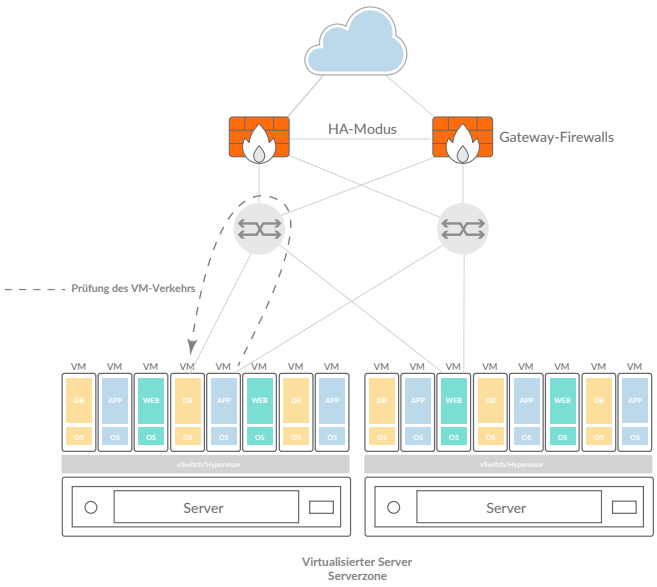

Abbildung 1: virtuelle Umgebung mit physischer Firewall

einer externen Firewall, die dann die Daten über denselben Kanal nach Süden leitet, zu führen. Dies würde allerdings viele Hops erfordern und kann Probleme wie Performanceeinbußen, hohe Latenz, Paketverluste und Schwierigkeiten bei der Sicherheitskontrolle (wie oben beschrieben) verursachen. Der zweite Ansatz ist die Nutzung einer softwarebasierten Firewall, die als Agent auf jeder VM ausgeführt wird. Diese Methode ist mit ähnlichen Herausforderungen verbunden: schlechte Performance und zusätzliche Verwaltungskomplexität bei steigender VM-Zahl.

Bei der Nutzung physischer Firewalls in einer dynamischen virtualisierten Umgebung steht die IT häufig vor folgenden Herausforderungen:

1. uneinsehbarer VM-to-VM-Datenverkehr
2. unkontrollierte Zunahme von Richtlinien
3. Virtual Sprawl
4. Public-Cloud-Umgebung

Uneinsehbarer VM-to-VM-Datenverkehr

Wenn Sie Dutzende VMs in einem virtuellen System haben, die untereinander kommunizieren, kann eine physische Perimeter-Firewall möglicherweise nicht den horizontalen Datenverkehr einsehen, weil der Verkehr aufgrund isolierter VMs oder Routing-Konfigurationen nie außerhalb dieses virtuellen Servers übertragen werden kann. Eine Überwachung des Verkehrs auf ungewöhnliche Ereignisse und Anomalien ist in solchen Szenarien nicht möglich.

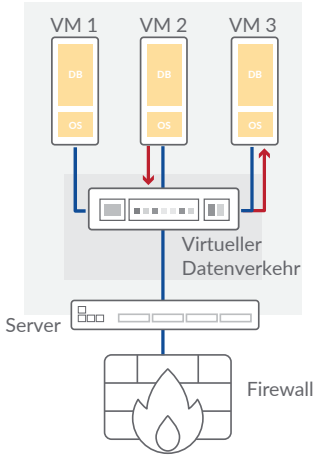

Abbildung 2: Datenverkehr zwischen virtuellen Maschinen

Unkontrollierte Zunahme von Richtlinien

Bei der Erstellung oder Verschiebung virtualisierter Ressourcen sind viele komplexe Änderungen der Netzwerkkonfiguration nötig, um den Datenverkehr dieser virtuellen Maschinen auf die physische Firewall zu lenken. Dies umfasst Routing- und NAT-Regeln, Ports und Protokolle, die von der Anwendung unterstützt werden. Changemanagement-Richtlinien sehen vor, dass Regeländerungen einen manuellen und aufwendigen Untersuchungs-, Genehmigungs-, Audit- und Test-Workflow durchlaufen, bevor sie in einer Produktionsumgebung eingeführt werden. Aufgrund seines hohen Personalbedarfs ist dieser Prozess höchst ineffizient, aufwendig und kostspielig.

Ein weiteres Problem: In vielen Organisationen gibt es wahrscheinlich schon unzählige andere undurchsichtige Regeln, die womöglich niemals geprüft und aussortiert wurden. Kommen weitere hinzu, werden die Sicherheitsregeln immer komplizierter und verschachtelter und lassen sich daher kaum noch verwalten. Das Ergebnis sind möglicherweise (größere) Lücken in den Richtlinien, nicht identifizierte Bedrohungen und/oder Performanceeinbußen.

Virtual Sprawl

Virtual Sprawl bezeichnet ein weitverbreitetes Problem, bei dem die Anzahl virtueller Ressourcen innerhalb einer Umgebung einen Punkt erreicht, an dem sie sich kaum noch nachvollziehen und kontrollieren lassen. Werden virtuelle Maschinen kopiert, geklont oder verlagert (oder, wie in vielen Fällen, außer Betrieb genommen und vergessen), kommt es zu Sicherheitsrisiken. Außerdem ist die Umgebung somit offen und anfällig für Angriffe, da Sicherheitsregeln und -kontrollen nicht mehr richtig funktionieren. Da sich die IP-Adressen virtueller Maschinen häufig ändern, ist eine feste Sicherheitsregel für eine VM-statische IP-Adresse unpraktisch. Dies ist ein häufiges Problem, das Hacker gerne ausnutzen. Dynamische virtuelle Umgebungen erfordern dynamische Sicherheitskontrollen sowie einen streng regulierten und prüfbaren Veränderungsprozess. Nur so kann sichergestellt werden, dass die virtuellen Maschinen die entsprechenden Sicherheits- und Konfigurationsregeln einhalten.

Public-Cloud-Umgebung

Problematisch ist auch, wenn sich die Anwendungsservices einer Organisation in der Public Cloud befinden, wie zum Beispiel Amazon Web Services (AWS) oder Microsoft Azure. In einer Cloud-Umgebung kann die IT-Abteilung keine physische Firewall-Appliance im geschützten Rechenzentrum des Providers platzieren, da es sich dabei um extrem kontrollierte Systeme handelt. Selbst wenn die IT ein physisches Gerät dort platzieren würde, könnte sie nicht das Verkehrsmuster bestimmen, sodass die Firewall sich vor dem Anwendungsverkehr der Organisation befinden würde. In diesem Fall ist eine virtuelle Firewall die beste Lösung. So kann die IT mittels Software-defined Networking (SDN) oder manueller Konfigurationen für Traffic-Engineering die virtualisierte Firewall zwischen ihren Anwendungsservices und dem Rest der Welt platzieren, unabhängig davon, ob dieser Pfad innerhalb oder außerhalb des Rechenzentrums verläuft.

Fazit

Wenn es um Virtualisierung geht, sollte der Sicherheitsaspekt eine wichtige Rolle bei der Kosten-Nutzen-Analyse spielen. Die Vorteile, wie Einsparungen und eine höhere Effizienz, müssen gegen mögliche Nachteile aufgrund wachsender Bedrohungen und häufiger Probleme abgewogen werden. Die IT muss über veraltete Ansätze und Technologien hinausgehen und sich mit neuen Lösungen befassen, die auf effiziente Weise die Sicherheit von Virtualisierungstechnologien gewährleisten.

Erfahren Sie mehr dazu: Lesen Sie unsere Lösungsübersicht Welche Funktionen eine virtuelle Next-Gen Firewall bieten sollte und besuchen Sie uns unter www.sonicwall.com/virtual-firewall.

Über uns

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

Wenn Sie Fragen zur Nutzung dieser Unterlagen haben, wenden Sie sich an:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, Kalifornien 95035, USA

Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com