UMFASSENDE SICHERHEIT IN DER CLOUD

Die rasche Einführung von Cloud-Technologien in Organisationen aller Grössen sorgt dafür, dass immer mehr Daten ausserhalb der traditionellen, standortabhängigen Sicherheitsmechanismen verlagert werden. Das Erreichen einer einheitlichen Sicherheitsstrategie in einem immer vielfältigeren und verteilten Netzwerk führt zu einer Menge neuer Herausforderungen.

→ **VON SONJA MEINDL**

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 ist der Datenverkehr anders: Workloads verlagern sich immer stärker in Richtung „Ost-West" – als Folge der Virtualisierung, der Shared Services und der neuen, verteilten Architekturen von Anwendungen.

„OST-WEST"-DATENVERKEHR SCHÜTZEN

In virtuellen Umgebungen kann die komplexe Kommunikation nur geringfügig 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 Gateway nicht passiert. Perimeter-Firewalls haben typischerweise nur sehr begrenzte Einblicke in den „Ost-West"-Datenverkehr. Das bedeutet, das Data Center ist angreifbar und Malware kann sich ungehindert ausbreiten.

SICHERHEITSLÖSUNGEN MÜSSEN SCHRITT HALTEN

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 – virtuellen Maschinen) 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.

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.

SICHERHEIT IN DER ÖFFENTLICHEN UND HYBRIDEN CLOUD

Eine zeitgemässe Security-Lösung muss durchgängige Sicherheit in öffentlichen und hybriden Cloud-Umgebungen sicherstellen. Sie muss umfassende Threat Prevention bei vollständiger Sichtbarkeit aller Bedrohungen in physischen wie virtuellen Umgebungen liefern und damit Organisationen bei der sicheren Migration in Cloud-basierte Umgebungen helfen. Die Unterstützung von allen gängigen Anbietern (z.B. AWS, Microsoft Azure, VMware, Cisco, OpenStack, Nuage Network, Google Cloud Platform, etc.) soll Unternehmen die Möglichkeit bieten, die Flexibilität und Kontrolle ihrer Netzwerke zu steigern, indem sie einen einheitlichen Rahmen, einheitliche Prozesse und Tools zur Anwendungsentwicklung sowie für die Sicherheit einführen.

Solch eine Lösung soll die mehrschichtige Sicherheit erweitern, um Daten und Assets in der Cloud vor Malware und anderen raffinierten Bedrohungen zu schützen. Ausgelegt auf dynamische und elastische Cloud-Umgebungen soll sie durch die Nutzung kontextbezogener Daten über VMs, Gruppen, Tags und anderen definierten Objekten die Richtlinien automatisch auf Änderungen in den Cloud-Umgebungen anpassen. Das führt zu verstärktem Schutz, der exakt auf die gezielten Anforderungen der Umgebung abgestimmt ist. Darüber hinaus soll sie nahtlos den Workloads und Daten von einer öffentlichen Cloud zur Stack-Umgebungen folgen und damit die eigenen Kontrollen des Cloud Providers ergänzen. Gleichzeitig muss sie einheitliche Sicherheitsrichtlinien, Durchsetzung, Logging- und Reporting ermöglichen - und das alles von einer einzigen, einheitlichen Management-Konsole aus.

DARAUF SOLLTEN SIE ACHTEN:

- Advanced Threat Prevention schützt Cloud-Assets vor externen und internen Bedrohungen und Gefahren. Sie sichert Traffic mithilfe umfassender, mehrschichtiger Sicherheitslösungen und ergänzt sowie komplementiert damit Cloud Provider-interne Kontrollen, indem es die Kommunikation mit dem Multi-Layer Security Ansatz absichert.
- Automatisierte und agile Security mit der Geschwindigkeit von DevOps und dynamischer Skalierung sowie Wachstum orientiert an Unternehmensanforderungen sorgen für operationelle Effizienz und ermöglichen eine elastische Geschäftsentwicklung. Die Lösung muss schnell ausgeliefert und bereitgestellt werden (durch Single-Click Provisionierung) On-Demand Bereitstellung und Nutzung-basierte Lizensierung (Pay-as-you-Grow model), die dazu führt, dass der TCO für Cloud Umgebungen verringert wird.
- „Single Pane of Glass" Sicherheitsmanagement für die öffentliche und private Cloud sowie für standortgebundene Netzwerke sorgt für einheitliches Richtlinienmanagement und Transparenz der gesamten Cloud-Infrastruktur.
- Sicherheitsrichtlinie, Logging und Reporting nutzen die vom Cloud-Provider definierten Objekte zur Verbesserung der Sichtbarkeit.
- Egal, welche Cloud, egal, welcher Service, immer sicher – wählen Sie eine umfassende Sicherheitslösung für Advanced Threat Prevention, und zwar für alle Cloud-Umgebungen – ob öffentlich, privat oder hybrid.

Check Point vSEC intergiert sich direkt in logische Netzwerke, schafft Transparenz und sichert den Datenverkehr virtueller Maschinen ab. Zudem überwacht die Lösung kontinuierlich alle Inhalte und erkennt Bedrohungen unmittelbar. vSEC verlängert die gleiche Multi-Layer Security, die Kunden in ihren eigenen Rechenzentren bereits haben, in die Cloud. ←

Dieser Beitrag wurde von der **Check Point Software Technologies** zur Verfügung gestellt und stellt die Sicht des Unternehmens dar. Computerworld übernimmt für dessen Inhalt keine Verantwortung.

Zur Autorin

Sonja Meindl ist diplomierte Wirtschafts-Ingenieurin und verantwortet als Country Manager seit 2012 die Geschäfte von Check Point in der Schweiz und in Österreich.

Zum Unternehmen:
Check Point Software Technologies ist der grösste Netzwerk-Cybersicherheitsanbieter weltweit und bietet branchenführende Technologien; schützt seine Kunden vor Cyberattacken mit einer unschlagbaren Fangquote bei Malware und anderen Bedrohungen. Check Point bietet eine umfassende Sicherheitsarchitektur, um Unternehmen zu schützen. Egal, ob Netzwerk oder Mobilgerät – Check Point deckt alle Bereiche ab und kann diese über seine leicht verständliche Sicherheitsmanagementplattform verwalten. Über 100'000 Organisationen aller Grössen vertrauen auf den Schutz von Check Point. Check Point Alps (Schweiz und Österreich) mit Sitz in Zürich und Wien beschäftigt rund 35 Mitarbeitende.

Mehr Informationen:
www.checkpoint.com

Check Point® SOFTWARE TECHNOLOGIES LTD.

Bild: Shutterstock/Jirsak

Eine zeitgemässe Security-Lösung muss durchgängige Sicherheit in öffentlichen und hybriden Cloud-Umgebungen sicherstellen.