Advertorial

Dynamische Sicherheit für alle Cloud-Szenarien

Gemischte Cloud-Umgebungen mit Private Cloud, Public-Cloud-Services und SaaS-Diensten bringen neue Sicherheitsanforderungen mit sich. Eine sogenannte «Security Fabric», die alle Sicherheitsaspekte unter einem Dach zusammenführt, eignet sich besser als herkömmliche Einzellösungen.

Cloud Computing ist längst Normalität. Die Marktforscher von IDC prognostizieren (Worldwide Quarterly Cloud IT Infrastructure Tracker), dass 2019 gegen 50 Prozent der weltweiten Ausgaben für IT-Infrastruktur auf Public- und Private-Cloud-Lösungen entfallen. 85 Prozent der Befragten gaben an, auf eine Multi-Cloud-Strategie zu setzen: Sie nutzen Cloud-Dienste für Infrastruktur (IaaS), Entwicklungsplattformen (PaaS), Softwareanwendungen (SaaS) sowie Cloud-Ressourcen in eigenen Rechenzentren in einem bedarfsgerecht adaptierbaren Mix.

Mit ihrer Security Fabric liefert Fortinet eine gesamtheitliche Sicherheit für dynamische Multicloud-Umgebungen.

Traditionelle Sicherheitslösungen stossen in einem derart virtualisierten und dynamischen Umfeld an ihre Grenzen. Eine gesamtheitliche Sichtbarkeit fehlt, verschiedene Lösungen kommunizieren schlecht untereinander, koordinierte Reaktionen auf Sicherheitsvorfälle sind nur schwer möglich und die Gesamtkosten für die Sicherheit sind enorm.

Eine Sicherheitsumgebung für die Cloud muss erstens alle Erscheinungsformen von Cloudlösungen (Private, Public, Hybrid) unter einem Dach erfassen und zweitens die Natur der Cloud als elastische, sehr schnell wandelbare Ressource nachvollziehen können. Dabei spielen drei Aspekte eine wichtige Rolle:

- **Skalierbarkeit:** Die Sicherheitslösung muss von Grund auf für dynamische Cloud-Workloads konzipiert sein. Statische und nicht automatisierbare Lösungen verhindern, dass die vollen Vorteile der Cloud zum Tragen kommen.
- **Konsistenz:** Cyberkriminelle nützen jede Schwachstelle aus – zum Beispiel inkonsistent aufgesetzte Policies. Mit der Cloud potenzieren sich solche Möglichkeiten. Die Sicherheitspolicies und deren automatisierte Durchsetzung müssen über alle statischen und dynamisch eingebundenen Ressourcen hinweg konsistent angewendet werden.
- **Segmentierung:** Um regulatorische Anforderungen zu erfüllen und das Geschäftsrisiko zu minimieren, müssen Systeme, Workloads und sogar spezifische Netzwerkkomponenten anhand ihrer Risikoprofile segmentierbar sein. So lassen sich der Datenfluss zwischen den Segmenten der Gesamt-Cloud überwachen und Datenverluste vermeiden.

Security Fabric statt Insellösungen

Die Security Fabric von Fortinet erfüllt diese Anforderungen. Die Fortinet-Sicherheitslösungen decken die verschiedensten Angriffsvektoren ab – in allen Umgebungen (vom IoT bis zur Cloud) – und ermöglichen die umfassende Erkennung und Abwehr von Cyberbedrohungen. Die FortiGate-Firewalls lassen sich über Konnektoren mit allen gängigen Public-Cloud-Anbietern und Private-Cloud-Umgebungen integrieren, sodass Informationen über «dynamische» Objekte, Security Templates oder Threat Intelligence nur einmal erfasst und danach in der gesamten Umgebung geteilt werden. Unterstützt werden sowohl Cloud-Plattformen wie AWS, Azure, Oracle und Google als auch SDN-Orchestrierungslösungen wie VMware NSX, Cisco ACI, Open Stack und Nuage Networks. Zudem sind die Produkte für alle gängigen Hypervisoren verfügbar. Fortinet pflegt und teilt Informationen innerhalb ihres Fabric Ready Programs mit verschiedenen Technologie- und Industriepartnern und unterstützt dabei auch behördliche Stellen wie Interpol oder die NATO Cybercrime Task Force.

Die Security-Fabric-Produkte bieten eine umfassende Programmierschnittstelle (API), die besonders der Automatisierung zugutekommt. Die API ermöglicht etwa die automatische Quarantäne auf Basis von Log-Events. Ein zentralisiertes Management und Reporting gewährleistet Transparenz in Echtzeit über die gesamte Multi-Cloud-Umgebung. Alle Lösungen können über eine moderne, einheitliche Weboberfläche verwaltet werden – im Gegensatz zu manch anderen Anbietern müssen auf den Workstations der Administratoren keine zusätzlichen Fat-Clients installiert werden.

Der Dynamik einer Cloud-Umgebung kommt entgegen, dass die Fortinet-Lösungen als virtuelle Appliances erhältlich sind. So können etwa Firewalls bei steigendem Workload dynamisch hinzugefügt oder Entwicklungsumgebungen nach der Produktionsaufnahme wieder zurückgefahren werden.

Fortinet Cloud Security: die Highlights

- Gesamtheitliche Sicherheit für dynamische Multicloud-Umgebungen
- Integration mit allen gängigen Public-Cloud-Providern, SDN-Orchestrierungsplattformen und Hypervisoren
- Sichere Einbindung von SaaS-Diensten wie Office 365 und Salesforce oder Cloud-Speicher-Lösungen via Cloud Access Security Broker Service (CASB)
- Umfangreiche APIs für vielfältige Automatisierung
- Lösungen als dynamisch skalierbare virtuelle Appliances erhältlich
- Starke Technologie- und Industriepartnerschaften via Fabric Reday Program

Kontakt

BOLL
IT Security Distribution
BOLL Engineering AG, Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60, info@boll.ch, www.boll.ch