CHECKLISTE

5 Herausforderungen bei der Datacenter-Sicherheit für hybride und Hyperscale-Rechenzentren und wie Sie sie mit Fortinet lösen

Die Weiterentwicklung von Rechenzentren bringt für Unternehmen zwar viele Vorteile, aber auch neue Sicherheitsprobleme mit sich – insbesondere bei der Umstellung auf hybride und Hyperscale-Architekturen. Fortinet bietet spezielle Lösungen für sicherheitsorientierte Netzwerke, die eigens für diese Herausforderungen entwickelt wurden. Unternehmen erhalten damit eine Security und Performance, die mit den einzigartigen Anforderungen einer hybriden und Hyperscale-Architektur mithalten kann.

Im Folgenden werden einige Fortinet-Lösungen für weitverbreitete Sicherheitsprobleme vorgestellt (mit Links zu ausführlichen Solution Guides).

1. HERAUSFORDERUNG: Begrenzte Transparenz

Die Umstellung vom klassischen Rechenzentrum auf eine hybride Architektur verändert Netzwerk- und IT-Infrastrukturen, die jetzt von On-Premises über Colocations bis hin zu mehreren Clouds alles abdecken. Diese Entwicklung geht jedoch oft zu Lasten der Netzwerk-Transparenz, was durch den Anstieg an verschlüsseltem Datenverkehr noch verschärft wird. Mit der falschen Lösung erhält das Unternehmen weder die notwendige Transparenz über alle implementierten Security-Elemente in den verschiedenen Umgebungen noch eine umfassende Sichtbarkeit und Kontrolle über Benutzer, Anwendungen und Geräte im Netzwerk.

Mit den FortiGate Network Firewalls lässt sich diese Transparenz sicher erreichen: Die Fortinet-Lösungen erkennen nicht genehmigte Anwendungen und versteckte Bedrohungen und konsolidieren wichtige Security-Funktionen wie Web-Filter und Bedrohungsschutz in einer einzigen Komplettlösung.

Weitere Informationen im Solution Brief

2. HERAUSFORDERUNG: Wachsende Angriffsfläche

In vielen Unternehmen fehlen angemessene interne Sicherheitskontrollen. Ressourcen werden nicht voneinander getrennt, wodurch Infektionen schnell überspringen und sich quer im Netzwerk verbreiten können. Die Lösung ist eine Segmentierung: Sie verhindert die seitliche Verbreitung von Bedrohungen, stärkt den Anwendungsschutz und trägt dazu bei, dass Unternehmen mit mehrstufigen Sicherheitskontrollen gesetzliche Vorgaben besser erfüllen können.

Fortinet-Lösungen schützen jede Art von Segmentierung – z. B. auf Netzwerk-, Port- und Anwendungsebene –, wenn der Datenverkehr von oder über eine FortiGate geleitet wird. Dank der flexiblen, leistungsstarken Funktionen für die Sicherheitsprüfung lässt sich dieser Schutz beliebig skalieren.

Weitere Informationen im Solution Brief

3. HERAUSFORDERUNG: Schwachstellen schützen

Ein Intrusion Prevention System (IPS) muss auch Sicherheit für hybride und Hyperscale-Rechenzentren bieten. Unternehmen brauchen ein vollständig integriertes IPS, um geschäftskritische, schwer zu patchende Altsysteme zu schützen und sie vor bekannten und Zero-Day-Bedrohungen abzuschirmen.

Mit den Fortinet Network Firewalls mit IPS können Sie Ihr bisheriges Netzwerk-Design beibehalten. Diese Firewalls werden von der Fortinet Security Fabric unterstützt, nutzen Bedrohungsdaten der FortiGuard Labs – gestützt durch künstliche Intelligenz (KI) und maschinelles Lernen (ML) – und bieten mit der FortiSandbox einzigartige On-Premises- und cloudbasierte Dienste, die unbekannte Bedrohungen verhindern. Sie bieten das beste Preis-Leistungs-Verhältnis und die höchste Wirksamkeit auf dem Markt, wie u. a. unabhängige Tests von den NSS Labs belegen.

Weitere Informationen im Solution Brief

4. HERAUSFORDERUNG: Hyperscale-Performance

Im Hyperscale-Zeitalter herrschen neue Anforderungen. Ob die ultraschnelle, sichere Übertragung riesiger Datenmengen ohne Performance-Einbußen oder extrem viele Benutzerverbindungen, ohne dass die Nutzererfahrung darunter leidet – können Netzwerk- und Security-Teams diese Bedürfnisse moderner Mitarbeiter und Kunden nicht erfüllen, leidet darunter die Produktivität und der gute Ruf des Unternehmens.

Hyperscale-Rechenzentren erfordern eine Hyperscale-Security, die sich mit Fortinet Network Firewalls realisieren lässt. Diese Firewalls arbeiten mit den neuesten Sicherheitsprozessoren, bieten eine unübertroffene Nutzer- und Anwendungserfahrung und haben das höchste Security Compute Rating der Branche – weil ihre Verbindungsleistung pro Sekunde gegenüber **12-mal** schneller als der Branchendurchschnitt ist. Fortinet Network Firewalls schaffen Datenübertragungen mit 10-facher Geschwindigkeit, haben eine **11-mal** leistungsstärkere IPSec-Verschlüsselung (sichere Hochleistungskonnektivität) und sind ideal für hardwaregestützte VXLANs, um hybride IT-Lösungen zu beschleunigen (z. B. das schnelle Aufrufen von Diensten).

Weitere Informationen im Solution Brief

5. HERAUSFORDERUNG: Management-Probleme

Durch immer größere, dezentralere Rechenzentren wird das Management zunehmend komplexer – besonders, wenn verschiedene Technologien und Konnektivitätspunkte spezielle Anforderungen haben, die sich nur mit mehreren Management-Tools erfüllen lassen.

Durch die Kombination von FortiManager und FortiAnalyzer im Fortinet Fabric Management Center (FMC) erhalten Sie ein effektives Network-Operations-Center (NOC) mit marktführenden FMC-Funktionen wie Reporting, Analysen, Automatisierung und ein zentrales Management. Die gesamte integrierte Security-Architektur wird transparent über eine einzige Konsole verwaltet und eignet sich auch für große Multivendor-Umgebungen. Drittlösungen wie Ansible (Automatisierung), Terraform (Automatisierung), ServiceNow (ITSM), Splunk (SIEM) und Tufin (NSPM) lassen sich problemlos im FMC integrieren.

Weitere Informationen im Solution Brief

FORTINET

www.fortinet.com/de

7. Dezember 2020, 11:21 Uhr

760844-0-1-DE