FORTINET

Dezentrale hybride Rechenzentren benötigen zusätzliche NGFW-Funktionen

Inhaltsverzeichnis

FORTINET

Zusammenfassung

Die Entwicklung moderner Rechenzentren hat dazu geführt, dass Anwendungen und Daten zunehmend auf hybride Infrastrukturen verteilt werden. Dies trägt zwar zu einer größeren Flexibilität für geschäftskritische Workflows bei, erweitert jedoch gleichzeitig die Angriffsfläche des Unternehmens und geht zu Lasten von Transparenz und Kontrolle. Netzwerk-Verantwortliche benötigen eine integrierte Security, die erweiterte Schutzfunktionen für hybride IT-Rechenzentrumsumgebungen bietet – insbesondere eine Next-Generation-Firewall (NGFW) mit leistungsstarken Funktionen für das kritische Risiko-Management, eine Skalierbarkeit der Security vom Rechenzentrum auf alle anderen Unternehmensbereiche, Ausfallsicherheit für einen kontinuierlichen Geschäftsbetrieb sowie Automatisierungs- und Orchestrierungsfunktionen, um Mitarbeiter zu entlasten und gleichzeitig Reaktionszeiten zu verkürzen.

Dezentrale Rechenzentren vergrößern die Angriffsfläche

Geschäftsanwender greifen heutzutage über zunehmend dezentrale Rechenzentren, die sich über eine hybride IT-Infrastruktur erstrecken, auf kritische Anwendungen zu. Workflows und Daten finden sich in unterschiedlichsten Umgebungen – von On-Premises und Colocations bis hin zu Private und Public Clouds. Diese weite Verteilung sensibler Inhalte führt jedoch dazu, dass die Angriffsfläche eines Unternehmens unablässig wächst.

Diesen wachsenden Risiken begegnen viele Netzwerk-Verantwortliche mit punktuellen Lösungen, um Sicherheitslücken zu schließen und neuen regulatorischen Vorgaben gerecht zu werden. Doch mit isolierten, schrittweise implementierten Einzellösungen lässt sich nicht das gesamte Spektrum heutiger und künftiger Schwachstellen abdecken. Stattdessen nimmt die Wahrscheinlichkeit von Geschäftsunterbrechungen infolge eines Cyberangriffs oder einer Naturkatastrophe zu, während gleichzeitig die Gesamtbetriebskosten (TCO) steigen und die Security zum Schutz des Unternehmens immer komplexer wird.

Die durchschnittlichen Gesamtkosten für Ausfallzeiten betragen über zwei Jahre umgerechnet rund 62,2 Millionen € pro Unternehmen, einschließlich Vertrauens- und Reputationsschäden.[1]

Security für hybride IT-Umgebungen

Um diese wachsende Angriffsfläche für Rechenzentren zu bewältigen, müssen Netzwerk-Verantwortliche zunächst die Sicherheit in sämtliche Bereiche ihrer hybriden IT-Umgebungen integrieren. Sie benötigen außerdem einen NGFW-Schutz, komplette Transparenz von Ende zu Ende, Richtlinienkontrollen und ein Intrusion Prevention System (IPS) sowie intelligente Funktionen für folgende Anforderungen:

- **Performance:** Für das Risiko-Management ist eine Security notwendig, die mit ultraschnellen Netzwerken Schritt halten kann. Auch werden robuste Funktionen benötigt, die effektiv zur Reduzierung der Angriffsfläche beitragen.
- **Ausfallsicherheit und Skalierbarkeit:** Werden hybride IT-Umgebungen erweitert und diversifiziert, muss die im Rechenzentrum eingesetzte Security auch Skalierbarkeit, Ausfallsicherheit und Verfügbarkeit bieten, um einen kontinuierlichen Geschäftsbetrieb sicherzustellen. Die gesamte Netzwerk- und Security-Architektur sollte zudem Störungen durch Netzwerkausfälle und Naturkatastrophen standhalten können.
- **Automatisierung und Orchestrierung:** Eine integrierte Security-Architektur bedeutet, dass die gesamte hybride IT-Infrastruktur von einer intelligenten Automatisierung profitiert. Automatisierte Sicherheitsreaktionen und schnellere Management-Funktionen verkürzen nicht nur die Dauer, die das Unternehmen einem Risiko ausgesetzt ist, sondern sorgen auch für eine Entlastung der Mitarbeiter, weniger menschliche Fehler und geringere Betriebskosten.

Zu den Hauptbedenken bei hybriden Daten-Workloads gehören: Datensicherheit/Einhaltung gesetzlicher Vorschriften (71 %), Leistung (62 %) und Einfachheit des Managements (53 %).[2]

Leistungsstarke Lösungen für das Risiko-Management

Rechenzentrums-Firewalls werden normalerweise im schnellsten Teil des Netzwerks bereitgestellt. Daher muss eine effektive NGFW-Lösung für solche Anwendungsfälle eine verbesserte L7-Sicherheit mit minimalen Auswirkungen auf die Netzwerkleistung bieten. **Spezielle Security-Prozessoren** sind dafür unverzichtbar. Nur so kann die NGFW die Sicherheitsfunktionen zuverlässig ausführen, ohne dass Netzwerk-Engpässe entstehen.

Die Sicherung eines modernen dezentralen Rechenzentrums erfordert auch Transparenz über alle bereitgestellten Security-Komponenten in sämtlichen Umgebungen (On-Premises, Colocations, Clouds usw.) sowie Transparenz über Benutzer, Anwendungen und Geräte. Da mittlerweile über ein Drittel (34 %) der Verstöße aus vertrauenswürdigen internen Quellen stammt,[3] kann es sich kein Unternehmen leisten, auf interne Zugangskontrollen zu verzichten. Netzwerk-Verantwortliche können den Zugang mit einer **Netzwerk-Segmentierung** regeln, die skalierbar und flexibel genug für unterschiedlichste Anwendungsfälle ist (einschließlich dynamischer Vertrauensstufen für Benutzer, Geräte und Anwendungen). Von Einzellösungen ist jedoch abzuraten, da die meisten keine der für die Segmentierung dringend benötigten Sicherheitsfunktionen wie eine Inhaltsinspektion bieten, die vor heutigen komplexen Bedrohungen schützen können. Eine NGFW für Rechenzentren muss für verschiedene Segmentierungstechniken anpassbar sein, Bedrohungsinformationen mit Sicherheitslösungen von Drittanbietern austauschen können sowie Funktionen – wie eine Inhaltsinspektion und einen automatisierten Bedrohungsschutz – umfassen.

Um mit dem Volumen und der Geschwindigkeit heutiger Bedrohungen Schritt zu halten, ist eine Security erforderlich, die Informationen in Echtzeit über eine integrierte Security-Architektur austauscht. Gleichzeitig sollten unbekannte Bedrohungen mithilfe künstlicher Intelligenz (KI) identifiziert werden können. Am wichtigsten ist dabei, dass diese **KI-gestützte Bedrohungserkennung und -abwehr** für sämtliche Ressourcen in allen Standorten funktioniert.

77 %

der Unternehmen verlassen sich derzeit bis zu einem gewissem Maße auf nicht integrierte, isolierte Sicherheitslösungen.[4]

Ausfallsicherheit und Skalierbarkeit

Digitale Innovationen bringen per se ständige Neuerungen mit sich, was sich direkt auf die Sicherheit auswirkt: Da die Workloads von Rechenzentren zunehmend über hybride IT-Infrastrukturen dezentral verarbeitet werden, muss die Security **schnell und einfach skalierbar** sein – Stichwort „Elastizität". Nur so lassen sich auch neue Anwendungen und wachsende Workloads abdecken. Diese Sicherheitsmaßnahmen müssen zudem über herkömmliche Geräte in Unternehmensstandorten (On-Premises) hinausgehen und auch alle Clouds sowie sämtliche implementierten virtuellen Maschinen (VM) effektiv schützen.

Die Sicherheit von Rechenzentren muss zudem an die Anforderungen eines ständig wachsenden Datenverkehrs anpassbar sein und sowohl unverschlüsselte als auch verschlüsselte Übertragungen kontrollieren können. Über 72 % des gesamten Netzwerk-Traffics besteht mittlerweile aus verschlüsselten Daten – ein Anstieg von fast 20 % gegenüber dem Vorjahr.[5] Größere verschlüsselte Verkehrsvolumen erfordern jedoch Tools zur HTTP- und HTTPS-Traffic-Inspektion, die eine erweiterte Transparenz bieten.

Dezentrale Rechenzentren sind besonders anfällig für Bedrohungen, die versteckt in verschlüsselten Datenströmen übertragen werden. Dagegen hilft nur eine Security mit einer intelligenten **SSL/TLS-Inspektion**, Sandbox und Decoy/Honeypot-Integration, die die gewaltigen Datenmengen bewältigen kann, die zwischen Benutzern und Systemen sowie zwischen Systemen übertragen werden – ohne die Anwendungsleistung zu beeinträchtigen. Diese Sicherheitslösung sollte mit den neuesten Inspektionsfunktionen (**TLS 1.3**) arbeiten.[6]

Was die Ausfallsicherheit und Verfügbarkeit betrifft, muss die Lösung bei einem Komponentenausfall ein Echtzeit-Failover des Systems sicherstellen. Ein integriertes **N+1 Clustering** bietet eine vollständig redundante Architektur, um Single-Point-of-Failures zu eliminieren. **Auch Validierungstests von unabhängigen Branchenexperten** tragen dazu bei, die Zuverlässigkeit der Lösung unter realen Bedingungen sicherzustellen.

60 %

des verschlüsselten Traffics enthält Malware[7] und 28 % der Datenpannen gehen auf Malware zurück.[8]

Automatisierung und Orchestrierung

Der anhaltende Fachkräftemangel im Bereich Cyber-Sicherheit erhöht die Arbeitsbelastung für ohnehin schon unterbesetzte Security-Teams. Wer die Betriebskosten in Grenzen halten und hochqualifizierte Security-Experten sinnvoll für Geschäftsziele und Optimierungen – statt für manuelle Routine-Aufgaben – einsetzen will, muss Betriebsabläufe vereinfachen. In dieser Hinsicht sollte eine effektive Firewall für Rechenzentren auch Funktionen umfassen, die z. B. **optimierte Workflows** für schlanke Implementierungs- und Management-Prozesse ermöglichen.

Eine integrierte Security-Architektur stellt die Grundlage für den Informationsaustausch und eine automatisierte Bedrohungsabwehr dar, um die Sicherheit in hybriden Infrastrukturen zu koordinieren. Zudem bietet eine NGFW-Lösung, die **offene APIs** unterstützt, entscheidende Vorteile wie die Workflow-Automatisierung, Orchestrierung und abgestimmte Sicherheitsreaktionen für ungepatchte Anwendungen und sich ständig ändernde DevOps-Umgebungen. Weiter sollte eine Sicherheitslösung die **Vertrauenswürdigkeit von Benutzern, Geräten und Anwendungen kontinuierlich anhand einer Geschäftslogik gewährleisten**, damit sich Sicherheitsprozesse (wie die Bereitstellung und Zugangskontrolle) leichter automatisieren lassen. Das entlastet nicht nur die Mitarbeiter, sondern senkt auch die Betriebskosten und verbessert zugleich die betriebliche Effizienz und die Sicherheitseffektivität.

Mit NGFW-Funktionen, die die **Automatisierung von Compliance-Berichten und Audit-Prozessen** vereinfachen, können Netzwerk-Verantwortliche auch die Aufgabenlast von Mitarbeitern reduzieren und zugleich mit sich ständig weiterentwickelnden Behördenvorgaben, Branchenvorschriften und Sicherheitsstandards wie NIST (National Institute of Standards and Technologies) oder CIS (Center for Internet Security) Schritt halten.

Für über die Hälfte der IT-Entscheidungsträger (54 %) ist der Fachkräftemangel einer der Gründe, die der Einführung eines hybriden Modells im Wege stehen.[9]

Empfehlung: Integrierte Security, ergänzt durch erstklassige NGFWs

Durch die Dezentralisierung von Rechenzentren und die Umstellung auf einen hybriden IT-Ansatz erweitert sich die Angriffsfläche eines Unternehmens. Trotz des steigenden Bedarfs an Rechenzentrumsleistung dürfen Netzwerk-Verantwortliche die Sicherheit nicht zugunsten der Erfüllung von Benutzeranforderungen aufs Spiel setzen. Angesichts der wachsenden Risiken und der immer höheren Wahrscheinlichkeit von Netzwerkausfällen müssen Unternehmen die Sicherheit moderner Rechenzentren neu bewerten.

Um sowohl die Security als auch die Performance sicherzustellen, brauchen Netzwerk-Verantwortliche eine integrierte Security-Architektur. Diese sollte auf einer robusten, leistungsstarken NGFW-Lösung basieren, die Ausfallsicherheit, Skalierbarkeit und Automatisierungsfunktionen bietet.

[1] Filip Truta: „Downtime Can Cost a Company up to $67 Million Over Two Years, Threatening Brand Reputation“. Security Boulevard, 21. Februar 2019.

[2] Alison DeNisco Rayome: „91 % of tech leaders say hybrid cloud is ‘ideal’ IT model“. TechRepublic, 15. November 2018.

[3] „2019 Data Breach Investigations Report“. Verizon, April 2019.

[4] „The CIO and Cybersecurity: A Report on Current Priorities and Challenges“. Fortinet, 23. Mai 2019.

[5] John Maddison: „Encrypted Traffic Reaches A New Threshold“. Network Computing, 28. November 2018.

[6] Alex Samonte: „TLS 1.3: What This Means For You“. Fortinet, 15. März 2019.

[7] Omar Yaacoubi: „The hidden threat in GDPR’s encryption push“. PrivSec Report, 8. Januar 2019.

[8] „2019 Data Breach Investigations Report“. Verizon, April 2019.

[9] Alison DeNisco Rayome: „91 % of tech leaders say hybrid cloud is ‘ideal’ IT model“. TechRepublic, 15. November 2018.

www.fortinet.com/de

Copyright © 2020 Fortinet, Inc. Alle Rechte vorbehalten. Fortinet®, FortiGate®, FortiCare® und FortiGuard® sowie bestimmte andere Marken sind eingetragene Marken von Fortinet, Inc. Bei anderen hier aufgeführten Namen von Fortinet kann es sich ebenfalls um eingetragene und/oder Gewohnheitsmarken von Fortinet handeln. Alle weiteren Produkt- und Unternehmensnamen sind u. U. Marken ihrer jeweiligen Eigentümer. Leistungs- und andere hierin enthaltenen Kennzahlen stammen aus internen Labortests unter idealen Bedingungen. Die tatsächliche Leistung und andere Ergebnisse können davon abweichen. Keine der hierin enthaltenen Angaben stellt eine verbindliche Verpflichtung durch Fortinet dar und Fortinet lehnt alle ausdrücklichen oder implizierten Garantien ab. Ausnahme: Fortinet geht einen verbindlichen, schriftlichen Vertrag mit einem Käufer ein, der vom Leiter der Rechtsabteilung von Fortinet unterzeichnet wird und der eine ausdrückliche Garantie dafür gewährt, dass ein bestimmtes Produkt entsprechend den genau angegebenen Leistungskennzahlen bestimmungsgemäß funktioniert. In diesem Fall sind ausschließlich die in diesem verbindlichen, schriftlichen Vertrag aufgeführten spezifischen Leistungskennzahlen für Fortinet bindend. Jede diesbezügliche Garantie beschränkt sich einzig auf die Leistung unter den gleichen idealen Bedingungen wie bei den internen Labortests von Fortinet. Fortinet lehnt dementsprechend jegliche ausdrücklichen oder implizierten Verpflichtungen, Zusagen und Garantien ab. Fortinet behält sich das Recht vor, diese Veröffentlichung ohne Ankündigung zu ändern, zu bearbeiten, zu übertragen oder anderweitig zu überarbeiten. Es gilt die jeweils aktuellste Fassung der Veröffentlichung.

472724-0-0-DE

5. Mai 2020, 15:32 Uhr