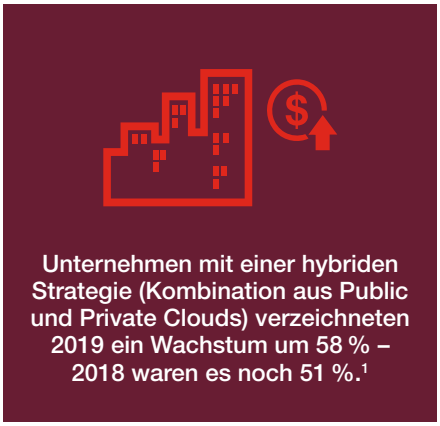
FORTINET

WHITEPAPER

Warum Rechenzentren für einen kontinuierlichen Geschäftsbetrieb keine ausreichende Security bieten

Zusammenfassung

Geschäftskritische Anwendungen werden mittlerweile zunehmend in dezentralen Rechenzentren gehostet, die sich über hybride IT-Infrastrukturen erstrecken – von On-Premises über Co-Locations bis hin zu Private und Public Clouds. Die Folge ist ein rasanter Anstieg bei standortübergreifenden digitalen Daten und Workflows. Dadurch wächst die Angriffsfläche des Unternehmens, während gleichzeitig weniger Transparenz und Kontrolle gegeben ist. Um diesem erhöhten Risiko zu begegnen, entscheiden sich viele Unternehmen für Security-Einzellösungen, die aber zu einer immer komplexeren Infrastruktur und mehr manuellen Abläufen für ohnehin schon überlastete Netzwerk- und Security-Teams führen. Die Folge ist eine Umgebung, die die operative Performance, die Zuverlässigkeit und die Verfügbarkeit beeinträchtigt und einen kontinuierlichen Geschäftsbetrieb gefährdet.



Unternehmen mit einer hybriden Strategie (Kombination aus Public und Private Clouds) verzeichneten 2019 ein Wachstum um 58 % – 2018 waren es noch 51 %.[1]

Wie sich eine wachsende Angriffsfläche auf Rechenzentren auswirkt

Aufgrund der zunehmenden Dezentralisierung moderner Rechenzentren verteilen sich anfällige Workflows und Daten auf eine hybride IT-Infrastruktur, die On-Premises, Co-Locations, Private Clouds und Public Clouds umfasst. Dadurch entsteht eine wachsende Angriffsfläche, die gesichert werden muss. Durch das Hinzufügen von Security-Einzelprodukten, um eine bestimmte Schwachstelle abzudecken oder Compliance-Anforderungen zu erfüllen, lässt sich jedoch dieses Problem nicht lösen. Netzwerk-Verantwortliche sind infolgedessen mit dem höheren Risiko eines erfolgreichen Cyber-Angriffs konfrontiert. Dadurch werden Netzwerk-Ausfälle aufgrund böswilliger Aktivitäten oder Naturkatastrophen wahrscheinlicher, während zugleich die operative Komplexität und die Kosten steigen.

Größeres Risiko

Sicherheitsrisiken im Rechenzentrum betreffen mehrere Aspekte:

Rechenzentren erstrecken sich auf mehrere Private und Public Clouds

Dezentrale Rechenzentren stellen immer mehr unterschiedliche cloudbasierte Dienste bereit. Dadurch werden Anwendungen und Daten innerhalb und außerhalb einer hybriden Infrastruktur bewegt, die von On-Premises bis hin zu Co-Locations und verschiedenen Arten von Clouds reicht. Herkömmlichen Sicherheitslösungen mit isolierten Ansätzen fehlt jedoch die Skalierbarkeit und Flexibilität, um die Anforderungen dieser neuen Hybridumgebung zu erfüllen. Netzwerk-Verantwortliche scheitern zunehmend an einem ortsunabhängigen Risiko-Management und dem Schutz kritischer Geschäftsanwendungen und dienste. Typische Gefährdungsszenarien sind z. B. sich schnell ändernde DevOps-Umgebungen oder wachstumsstarke E-Commerce-Unternehmen. Insbesondere mangelt es bei Sicherheitsstrategien an Transparenz über den Netzwerk-Traffic und Netzwerk-Elemente. Auch eine intelligente Erkennung und Abwehr von unbekannten Gefahren und Zero-Day-Bedrohungen sind selten vorhanden.

Malware-Verschlüsselung

Nie zuvor wurden so viele Daten verschlüsselt im Netzwerk übertragen: Mittlerweile sind es über 72 % des gesamten Netzwerk-Traffics – ein Anstieg von fast 20 % gegenüber dem Vorjahr.[2] Im vergangenen Jahr gingen 28 % der Sicherheitsverletzungen auf Malware zurück.[3] Diese Schadsoftware wird häufig „getarnt“ durch die SSL-Verschlüsselung (Secure Sockets Layer) oder TLS-Verschlüsselung (Transport Layer Security) ins Unternehmensnetzwerk eingeschleust. Wie Studien zeigen, wird bei über 60 % der Angriffe Malware mit der SSL- oder TLS-Verschlüsselung verschleiert.[4] Dazu gehört Malware wie Zeus, TrickBot oder Dridex, eine Schadsoftware zur Aufzeichnung von Tastatureingaben, mit der Hacker an wertvolle Anmeldedaten (wie Passwörter für Bankkonten) gelangen und großen finanziellen Schaden anrichten können.

Die meisten Firewalls bremsen die Netzwerk-Performance erheblich aus, wenn die Überprüfung von SSL- und TLS-Traffic bei Firewalls aktiviert ist. Um diesen Leistungsverlust aufzufangen, müssen Netzwerk-Verantwortliche entweder mehr Firewalls oder separate Geräte für die SSL-/TLS-Inspektion anschaffen. Diese Optionen haben jedoch höhere Investitions- und Betriebskosten zur Folge, da der Management-Aufwand durch die zusätzlichen Lösungen erheblich steigt. Viele Unternehmen stehen daher vor der schwierigen Frage, ob trotz der Mehrkosten und Leistungseinbußen eine SSL- und TLS-Inspektion erfolgen soll – oder ob man auf die Überprüfung von verschlüsseltem SSL- und TLS-Datenverkehr zugunsten der Performance vollkommen verzichtet. Weitere Faktoren, die die Umstellung auf eine SSL- und TLS-Inspektion erschweren, sind Datenschutzprobleme und das oft als schwierig empfundene Zertifikat-Management.

Mangelnde Transparenz und Kontrolle

34 % der Sicherheitsverletzungen gehen mittlerweile auf vertrauenswürdige interne Quellen zurück.[6] Transparenz und Zugriffskontrollen im internen Netzwerk sind folglich ein Muss. Schließlich kann eine Segmentierung von Benutzern, Geräten, Anwendungen und Diensten dazu beitragen, einen unbefugten Zugriff auf vertrauliche Inhalte zu verhindern. Das Problem ist jedoch, dass eine herkömmliche netzwerkbasierte Segmentierung keine inhärenten Mechanismen für die Inhaltsprüfung bietet. Die Folge: Ist Malware erst einmal ins Netzwerk gelangt, kann sie sich ungehindert verbreiten.

Statische Vertrauensstufen spiegeln nicht die Realität wider – ob beim Benutzerverhalten oder bei Geschäfts- und Produktivitätsanforderungen. Vertrauenswürdige Benutzer können unwissentlich einen Virus einschleusen oder kompromittierte Anmeldedaten verwenden und so den Diebstahl von Daten ermöglichen – ganz zu schweigen von Situationen, in denen Benutzer Zugriffsrechte vorsätzlich missbrauchen, um Informationen in böswilliger Absicht zu stehlen. Auch Geräte und Anwendungen, die einmal als „sicher" eingestuft wurden, können irgendwann infiziert werden. Leider fehlt es den meisten Unternehmen an umfassender Transparenz und richtlinienbasierten Zugriffskontrollen, um Angriffe aus dem Inneren des Netzwerks zu verhindern.

90 % der Unternehmen haben einen Netzwerk-Angriff infolge von SSL- oder TLS-verschlüsselter Schadsoftware erlebt oder rechnen damit.[5]

Die überwiegende Mehrheit (89 %) der Sicherheitsverantwortlichen in großen Unternehmen hat immer noch Probleme mit der Transparenz und dem Einblick in vertrauenswürdige Daten.[7]

Netzwerk-Ausfälle

Ausfallsicherheit und Verfügbarkeit von Rechenzentren sind für den operativen Erfolg entscheidend. Angesichts des Anstiegs bei Daten und Workloads – infolge von IoT-Geräten (Internet der Dinge), Big-Data-Analytics und künstlicher Intelligenz (KI) – benötigen Unternehmen eine Security, die mit dem Wachstum und der Entwicklung ihres Netzwerk-Traffics Schritt halten kann. So wird bis 2021 für den weltweiten IP-Datenverkehr eine durchschnittliche jährliche Wachstumsrate (CAGR) von 26 % über fünf Jahre prognostiziert. Bei der Bandbreite von Verbindungen (für den internen Datenaustausch zwischen Unternehmen) wird zudem ein Anstieg um 48 % erwartet.[8]

Diese Größenordnung des digitalen Wachstums erhöht die Wahrscheinlichkeit eines erheblichen Netzwerk-Ausfalls, der das Unternehmen ernsthaft schädigt. Ein durchschnittlicher Infrastrukturausfall kann pro Stunde über 100.000 US-Dollar kosten, ein Ausfall kritischer Anwendungen kann sogar mit 500.000 bis 1 Million US-Dollar pro Stunde zu Buche schlagen.[9]

Die Wahrscheinlichkeit eines kritischen Infrastrukturausfalls steigt auch bei Cyber-Angriffen und Naturkatastrophen. Mögliche Folgen sind Betriebsstörungen oder Ausfallzeiten, eine schlechte Nutzererfahrung, Image-Schäden, Datendiebstahl und Umsatzverluste. Erdbeben, Überschwemmungen und Brände können zu durchtrennten Glasfaserleitungen, Stromausfällen und zum Versagen der Kühlsysteme führen und kritische Dienstausfälle in Rechenzentren nach sich ziehen. Aber auch Katastrophen wie Unfälle mit Baugeräten oder andere menschliche Fehler können ähnliche Probleme verursachen.

Kosten und operative Komplexität

Als Reaktion auf die wachsende Angriffsfläche greifen viele Unternehmen zu isolierten Einzellösungen, um Lücken bei der Bedrohungsabwehr zu schließen. Doch dieser Ansatz ist nicht nur ineffizient und kostspielig, sondern erhöht auch die Komplexität der Infrastruktur erheblich – was die Sicherheitseffektivität zusätzlich schwächt.

Die Verbreitung von Security-Einzelprodukten ist ein ernstes Problem: In einem durchschnittlichen Unternehmen gibt es 75 verschiedene Sicherheitslösungen, von denen viele nur für eine einzige Schwachstelle oder Compliance-Anforderung installiert wurden.[10] Mehr als drei Viertel (77 %) der Unternehmen verlassen sich in gewissem Umfang auf nichtintegrierte Security-Einzellösungen, wodurch das Netzwerk für Cyber-Angriffe anfällig wird.[11] Da diese unterschiedlichen Produkte in der Regel keine Bedrohungsdaten austauschen oder Reaktionen in einer zunehmend dezentralen, hybriden IT-Infrastruktur koordinieren können, verlängern sich die Reaktionszeiten auf Sicherheitsvorfälle. Dadurch erhöht sich wiederum die Wahrscheinlichkeit, dass kritische Systeme infiziert werden oder nicht mit voller Leistung laufen – bis hin zum Totalausfall und dem Diebstahl wertvoller Daten.

Die Verbreitung von isolierten Sicherheitslösungen erfordert zudem mehr manuelle Workflows. Manuelle Prozesse beeinträchtigen jedoch die Skalierbarkeit und Flexibilität der Security und führen zu uneinheitlichen Sicherheitsrichtlinien für On-Premise- und Cloud-Umgebungen. Dieses Problem wird durch manuelle Workflows für Compliance-Tracking, -Audits und -Berichte noch verstärkt. Dazu kommt, dass Branchenstandards und datenschutzrechtliche Anforderungen von Jahr zu Jahr komplexer werden. Ohne eine Automatisierung der Security steigt dadurch die Belastung für ohnehin unterbesetzte IT-Teams um ein Weiteres – und auch das Risiko behördlicher Bußgelder aufgrund menschlicher Fehler.

Weiterentwicklung der Security für Rechenzentren

Mit zunehmender Verteilung von Rechenzentren auf eine hybride IT-Infrastruktur vergrößert sich die Angriffsfläche eines Unternehmens erheblich. Inkonsequente Sicherheitskonzepte können mit diesen wachsenden Risiken nicht Schritt halten und erhöhen die Wahrscheinlichkeit von Netzwerk-Ausfällen – ganz zu schweigen von den Kosten und der Komplexität, die die Aufrechterhaltung einer zerklüfteten Sicherheitsarchitektur angesichts wachsender Bedrohungen mit sich bringt.

Infolge des Fachkräftemangels im Bereich Cyber-Sicherheit sind heute weltweit fast 3 Millionen Security-Positionen unbesetzt.[12]

Netzwerk-Verantwortliche sollten die derzeitige Absicherung moderner Rechenzentren neu bewerten und sich folgende Fragen stellen:

- Verbessert die Lösung die Sicherheitstransparenz für alle Security-Elemente?
- Überprüft sie den gesamten Netzwerk-Traffic – verschlüsselten und unverschlüsselten?
- Bietet sie – unabhängig vom Standort digitaler Ressourcen – eine erweiterte Bedrohungserkennung und -abwehr?
- Unterstützt sie Hochverfügbarkeit und Ausfallsicherheit mit N+1-Redundanz-Clustern für nahtloses, virtuelles Failover in Echtzeit bei Naturkatastrophen oder Angriffen?
- Unterstützt sie eine absichtsbasierte Segmentierung mit dynamischen Vertrauensstufen für Benutzer, Geräte und Anwendungen?
- Funktioniert sie als Teil einer integrierten Security-Architektur mit automatisierter Weitergabe von Bedrohungsinformationen und -reaktionen an alle bereitgestellten Sicherheitselemente?

[1] „RightScale 2019 State of the Cloud Report from Flexera Identifies Cloud Adoption Trends“. RightScale/Flexera, 27. Februar 2019.

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

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

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

[5] Ebd.

[6] „2019 Data Breach Investigations Report“. Verizon, April 2019.

[7] „Why poor visibility is hampering cybersecurity“. Help Net Security, 24. Juni 2019.

[8] Tom Coughlin: „Bandwidth Growth Drives Storage Demand“. Forbes, 24. September 2018.

[9] Kevin O'Connor: „Is Your Disaster Recovery Plan Up to Date?“. CIO, 18. April 2016.

[10] Kacy Zurkus: „Defense in depth: stop spending, start consolidating“. CSO Online, 14. März 2016.

[11] „CISOs und Cyber-Security: Ein Bericht über aktuelle Prioritäten und Herausforderungen“. Fortinet, 23. Mai 2019.

[12] „Cybersecurity Skills Shortage Soars, Nearing 3 Million“. (ISC)², 18. Oktober 2018.

FORTINET

www.fortinet.com/de

Dezember 17, 2019 11:26 vorm.

452531-0-1-DE