FORTINET

WHITEPAPER

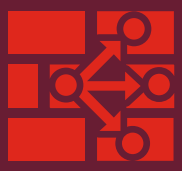
SD-WAN im Zeitalter der digitalen Innovation

Geschäftliche Agilität erreichen und Störungen minimieren

Zusammenfassung

Der Großteil der Unternehmen implementiert derzeit digitale Innovationen (DI), um mit neuen Technologien bestimmte Ziele zu erreichen und Kunden so einen höheren Mehrwert zu bieten. Aber digitale Innovationen sind oft auch ein Störfaktor, da sie mit einer erweiterten Angriffsfläche und einer komplexeren Bedrohungslage einhergehen. Nicht selten wird die Security immer komplizierter, wenn versucht wird, neuen Gefahren mit punktuellen Sicherheitslösungen Herr zu werden. Auch die Einhaltung wichtiger Industrie- und Regulierungsstandards wie der Datenschutz-Grundverordnung (DSGVO) wird dadurch erheblich erschwert.

Trotz dieser Probleme hat sich eine wichtige digitale Innovation schnell durchgesetzt: die SD-WAN-Technologie. Wie die Praxis zeigt, ist das SD-WAN – die Abkürzung steht für „Software-Defined Wide Area Network" – leider oft ein Paradebeispiel für das Paradoxon digitaler Innovationen: Transformative Technologie kann neue Geschäftserfolge bringen, aber zugleich das Risiko durch die technologiebedingte erweiterte Angriffsfläche erhöhen. Die Herausforderung besteht darin, das SD-WAN zu nutzen und gleichzeitig potenzielle Störfaktoren auszugleichen, die damit oft einhergehen.



Digitale Innovationen bringen mehr Dienste in die Cloud, wodurch herkömmliche Netzwerk-Architekturen überlastet und Unternehmen dazu gebracht werden, ein SD-WAN einzuführen.

Parallele digitale Innovationen

Auch wenn die Verlagerung von Workloads und Infrastrukturen in unzählige Public Clouds mittlerweile kaum noch als digitale Innovation gilt, ist und bleibt ihr Einfluss auf die Betriebsabläufe eines Unternehmens gewaltig. Schließlich beschert die umfassende Nutzung von Public Clouds dem Unternehmen agilere Arbeitsweisen und eine schnellere Skalierbarkeit.

Wie ein Unternehmen Public Clouds konkret nutzt, mag sich von Fall zu Fall unterscheiden, wird aber meistens durch eine Gemeinsamkeit gekennzeichnet: die hybride Architektur der Cloud-Lösung. Da sich eine Anwendung zu jedem Zeitpunkt an einem beliebigen Ort befinden kann – On-Premises oder in der Public Cloud – und problemlos zwischen diesen beiden Umgebungen wechseln kann, führt der Agilitätsvorteil der Public Cloud für das Netzwerk-Operations-Team nicht selten zu erheblichen Problemen beim WAN-Management.

SD-WAN – die Lösung zur Vermeidung von Netzwerk-Störungen durch digitale Innovationen

Mit der Verlagerung von mehr und mehr Diensten in die Cloud wird immer deutlicher, dass „herkömmliche Netzwerk-Architekturen ... nicht für die Workloads einer Cloud-First-Organisation ausgelegt sind".[1] Dies hat zu einem rasanten Wachstum einer weiteren wichtigen DI-Technologie geführt – dem SD-WAN. „Rasant" ist hier das Stichwort: Untersuchungen von IHS Markit zeigen, dass 74 % der Unternehmen 2017 SD-WAN-Tests durchgeführt und im Folgejahr implementiert haben.[2]

Ein SD-WAN bietet Benutzern in Remote-Standorten einen leistungsstarken Zugriff auf Cloud-Anwendungen und ermöglicht ein agileres Netzwerk sowie die Automatisierung in Filialen in einem bisher nicht möglichen Umfang. Besondere Vorteile sind beispielsweise:

1. **Direkter Cloud-Zugriff:** Ein SD-WAN macht das Backhauling – das Routing des gesamten Cloud- und Filialverkehrs durch das Rechenzentrum – überflüssig. Stattdessen können alle Anwender unabhängig vom Standort direkt auf kritische Cloud-Dienste zugreifen.
2. **Bessere Anwendungsleistung:** Ein SD-WAN kann so konfiguriert werden, dass geschäftskritischer Datenverkehr und Echtzeit-Dienste wie Voice over Internet Protocol (VoIP) höhere Priorität erhalten und über die effizienteste Route geleitet werden. Wenn mehrere Optionen für den Datenverkehr bestehen, können Paketverluste durch überlastete Leitungen und Latenzzeiten aufgrund von starkem Datenverkehr reduziert und die Leistung und Nutzererfahrung verbessert werden.[3]
3. **Höhere geschäftliche Agilität:** Netzwerkplaner müssen nicht mehr Wochen oder Monate im Voraus die Bereitstellung zusätzlicher MPLS-Bandbreite (Multiprotocol-Label-Switching) bedenken, wie es bei einem herkömmlichen WAN notwendig ist. Zudem wird ein schnelles Vorankommen von digitalen Innovationen nicht mehr dadurch behindert, dass die Netzwerkleistung an mehreren Standorten sichergestellt werden muss.
4. **Kostensenkungen:** Ein SD-WAN ermöglicht die effiziente Weiterleitung des Datenverkehrs über mehrere Kanäle – nicht nur über bestehende MPLS-Schaltungen, sondern auch über das öffentliche Internet per LTE und Breitband. Dies senkt die Kosten für neue MPLS-Bandbreite.

Ein SD-WAN kann auch die Netzwerk-Security beeinträchtigen

Gegen die Vorteile einer SD-WAN-Netzwerkarchitektur in einer Welt der digitalen Innovationen ist schwerlich etwas einzuwenden. Aber ein SD-WAN hat auch einen eklatanten Nachteil: Jeder SD-WAN-fähige Standort mit lokalem Internetzugang ist eine zusätzliche Ausweitung der Angriffsfläche und eine weitere Schwachstelle in der Netzwerk-Sicherheitskette. Dies verschärft ein bestehendes Problem, da das Sicherheitsniveau von Zweigniederlassungen oft schon vor der SD-WAN-Einführung niedriger war als in der Zentrale.

Natürlich wird die Angriffsfläche eines Unternehmens auch von den meisten anderen DI-inspirierten Technologie-Implementierungen vergrößert, und die Sicherheit gilt oft als die größte Barriere für diese Initiativen.[5] Um erfolgreich zu sein, muss jede DI-Initiative – auch eine SD-WAN-Implementierung – eine realistische Bewertung ihrer Auswirkungen auf die Sicherheit und die proaktive Behebung potenzieller Probleme umfassen, bevor die eigentliche Implementierung erfolgt.

74 % der Unternehmen haben 2017 SD-WAN-Tests durchgeführt und SD-WAN-Lösungen im Folgejahr implementiert.[4]

Ein SD-WAN erfordert das Überdenken langjähriger Grundsätze der Security für Unternehmen, einschließlich des Schutzes des Perimeters.

Effektiver Schutz für ein SD-WAN

Security für digitale Innovationen beinhaltet das Überdenken langjähriger Prinzipien der Unternehmenssicherheit – einschließlich des perimeterbasierten Modells, das mit jeder Einführung eines weiteren Cloud-Dienstes an Effektivität verliert und für ein SD-WAN völlig unbrauchbar ist. Notwendig ist auch, dass die Sicherheit ein integraler Bestandteil der DI-Planung und nicht ein nachträglicher Gedanke ist. Bei jeder digitalen Initiative sollten Planungs- und Implementierungsteams den Grundsatz „Security by Design, Security by Default“ befolgen.

Bei der SD-WAN-Implementierung sollten Netzwerk-Security- und Netzwerk-Operations-Teams am Entscheidungsprozess für eine Lösung beteiligt sein. Auch sollte zu dem Zeitpunkt, wo mehrere Sicherheitslösungen in die engere Wahl genommen werden und die Kaufentscheidung getroffen wird, bereits eine Sicherheitsstrategie vorhanden sein. Diese Teams arbeiten traditionell in Silos und stehen manchmal in leichter Konkurrenz zueinander.[6] Arbeiten beide Teams aber zusammen, können sie die legitimen Sicherheitsbedenken rund um ein SD-WAN strategisch angehen:

- Sicherung der erweiterten Angriffsfläche, die durch digitale Initiativen und die SD-WAN-Infrastruktur geschaffen wurde
- Sicherstellung, dass ins Netzwerk eingeschleuste Malware sich nicht horizontal verbreitet
- Kompensation von fehlenden qualifizierten IT-Teams an einigen entfernten Standorten
- Bereitstellung netzwerkweiter Transparenz und zentralisierter Sicherheitskontrollen für das gesamte Unternehmen

Integration – der Schlüssel zum Erfolg beim SD-WAN

In einer Umfrage verzeichnete das typische Unternehmen über einen Zeitraum von zwei Jahren 20 unbefugte Zugriffe im Zusammenhang mit Cyber-Angriffen, von denen vier zu Verstößen mit resultierenden Schäden wie Datenverlust oder Ausfallzeiten bzw. zu einem Compliance-Ereignis führten.[7] Die meisten davon sind komplexe Bedrohungen, die darauf abzielen, herkömmliche Sicherheitsmaßnahmen zu umgehen. Werden das SD-WAN und andere digitale Initiativen nicht strategisch implementiert, können sie diese Bedrohungen sogar noch verstärken.

Bei der SD-WAN-Implementierung müssen Unternehmen sicherstellen, dass die Security ein Teil der Gleichung ist: Da der Netzwerkverkehr das Rechenzentrum umgeht, muss die Netzwerk-Sicherheitsarchitektur erweitert werden – nicht jedoch durch das Hinzufügen von Silos zur Sicherheitsarchitektur. Mit einer wirklich sicheren SD-WAN-Lösung ist die Sicherheit im Netzwerk integriert und erstreckt sich über eine multinationale, verteilte Unternehmensumgebung, was zentrale Transparenz und Kontrolle, echte Automatisierung von Sicherheitsprozessen, die dynamische Weitergabe von Bedrohungsinformationen und ein robusteres Netzwerk ermöglicht.

Wie das SD-WAN ein Erfolg wird

Ein SD-WAN eröffnet Unternehmen eine großartige Möglichkeit, in den Filialnetzen für spürbaren Mehrwert zu sorgen. Zu den Dingen, an die IT- und Security-Experten denken müssen, zählen beispielsweise:

- Das SD-WAN ist für viele Unternehmen ein wichtiges Bindeglied.
- Der Geschäftswert eines SD-WANs ist spürbar, da es die Bereitstellung von Cloud-Diensten für Zweigniederlassungen erleichtert, die Anwendungsleistung und die Agilität des Unternehmens erhöht und die Kosten senkt.
- Ein SD-WAN vergrößert die Angriffsfläche und kann in vielen Unternehmen das schwächste Glied in der Sicherheitskette sein.
- Die Security muss ein zentrales Element jeder SD-WAN-Implementierung sein.
- Integration ist entscheidend, wenn es um die Sicherheit des SD-WANs geht.

20 unbefugte Zugriffe nach Cyber-Angriffen mussten typische Unternehmen in den letzten Jahren verzeichnen. Da die Zugriffe erst nach über 6 Monaten erkannt wurden, bröckelt das traditionelle Sicherheitsparadigma und Unternehmen sind Datendiebstahl, Ransomware und Betriebsausfällen ausgesetzt.

[1] Kelly Ahuja: „A Digital-first Enterprise Needs SD-WAN“. Network World, 7. Juni 2018.

[2] Andy Patrizio: „Enterprises Are Moving to SD-WAN Beyond Pilot Stages to Development“. NetworkWorld, 7. Mai 2018.

[3] Lee Doyle: „How Does SD-WAN Manage Real-time Network Performance?“ TechTarget SearchSDN, 9. Januar 2018.

[4] Andy Patrizio: „Enterprises are moving to SD-WAN beyond pilot stages to development“. Network World, 7. Mai 2018.

[5] „Security Implications of Digital Transformation Report“. Fortinet, 26. Juli 2018.

[6] Erin O'Malley: „Driving the Convergence of Networking and Security“. SecurityWeek, 15. Mai 2018.

[7] “Security Implications of Digital Transformation Report“. Fortinet, 26. Juli 2018.

FORTINET

www.fortinet.com/de

29. Juni 2020 10:58 Uhr

253349-B-1-DE