aruba
a Hewlett Packard Enterprise company

EBOOK

Vereinheitlichte Infrastruktur und schnellere Geschäftsabläufe

Fünf Vorteile eines vereinheitlichten Netzwerks

Vereinheitlichen Sie Ihre Infrastruktur mit cloudverwaltetem Networking

Die Cloud bietet erwiesenermaßen Vorteile für Unternehmen. Die Modernisierung der IT durch Cloud-Apps, Cloud-Computing und Cloud-Speicherung hat zu einer besseren Zusammenarbeit, schnelleren Innovationen und mehr Kosteneffizienz in sämtlichen Unternehmensabteilungen geführt.

Als Nächstes wandern die Netzwerke in die Cloud. Durch die zunehmende Anzahl von Remote-Mitarbeitern und IoT-verbundenen Geräten wird die Verwaltung herkömmlicher Netzwerke zu kompliziert. Diese Komplexität wird durch die unabhängige Verwaltung von WAN-, kabelgebundenen und drahtlosen Netzwerken noch verstärkt, die von eigenständigen Tools orchestriert werden. Die Herausforderungen, die dadurch entstehen, können Ausfallzeiten und zweifelhafte Benutzererfahrungen verursachen.

Silos können jedoch aufgelöst werden und das Netzwerkmanagement lässt sich vereinfachen: durch einen vereinheitlichten Netzwerkbetrieb in der Cloud. Eine einheitliche Infrastruktur konsolidiert das Management aller Netzwerke – in einem einzigen, cloudnativen Dashboard.

50% der neu bereitgestellten Netzwerke werden bis 2022 über cloudbasierte Plattformen verwaltet werden.[1]

42% der Unternehmen planen die Einführung von SD-WAN oder haben es bereits eingeführt, um die IT-Agilität und die Bereitstellung von Cloud-Apps zu verbessern.[2]

30% der Unternehmen werden bis 2023 KI-fähige Tools einführen, um herkömmliche Überwachungsansätze zu erweitern, das sind 2 % mehr als heute.[3]

1. IDC, “Five Key Enterprise Networking Trends to Watch in 2020,” April 2020
2. Ibid
3. Gartner, “Use AIOps for a Data-Driven Approach to Improve Insights from IT Operations Monitoring Tools,” May 2020

1 Dank verbesserter Netzwerk-Agilität mit digitalen Innovationen Schritt halten

Die digitale Transformation hat Fahrt aufgenommen. Unternehmen erhoffen sich Wettbewerbsvorteile, wenn sie ihre Lieferketten optimieren, überzeugende Erlebnisse für Kunden und Mitarbeiter schaffen oder sogar ganz neue Geschäftsmodelle einführen. Fast 60% der geschäftlichen Interaktionen laufen heute digital ab, 2019 waren es 36%[1].

Netzwerke werden auch weiterhin eine zentrale Rolle bei der Bereitstellung von Anwendungen, Daten und den daraus resultierenden digitalen Erlebnissen für die Endbenutzer spielen. Leider stehen veraltete, isolierte und manuell verwaltete Netzwerke den Unternehmen im Weg.

Es ist zeitraubend, mühselig und kostspielig, wenn notwendige Änderungen am Netzwerk Gerät für Gerät vorgenommen werden müssen. Manuelle Vorgänge dieser Art erfordern kostspielige Fahrten, um qualifizierte IT-Mitarbeiter von einem Standort zum nächsten zu bringen, und führen oft zu Verzögerungen, Budgetüberschreitungen und Bedienerfehlern.

[1]*Quelle: McKinsey & Company*

Manuelle Netzwerkabläufe bergen höheres Fehlerrisiko

26%

der Netzwerkprobleme werden durch menschliche Fehler verursacht.

EMA, Network Management Megatrends, 2020

Demgegenüber erleichtern in der vereinheitlichten Cloud verwaltete Netzwerke die Bereitstellung neuer Dienste und sogar ganz neuer Standorte erheblich. Mithilfe von Funktionen wie der voll automatisierten Bereitstellung kann die IT Geräte wie Access Points, Switches und Gateways vorkonfigurieren. Wenn die Geräte am Zielort eintreffen, müssen sie nur angeschlossen und eingeschaltet werden. Konfigurationen und Richtlinien beziehen sie dann aus der Cloud. So ist die Netzwerkkonnektivität innerhalb von wenigen Minuten eingerichtet und betriebsbereit.

Eine ähnliche Effizienz kann auch während der Zeitfenster für Änderungen erzielt werden. Die IT kann Konfigurationsänderungen einmalig in einer cloudbasierten Managementkonsole vornehmen, unmittelbar überprüfen, ob diese Aktualisierungen den Netzwerkrichtlinien entsprechen und fehlerfrei sind, und die neuen Einstellungen dann sofort auf alle entsprechenden Geräte im Netzwerk übertragen.

Cloudgestützte Arbeitsabläufe wie diese ermögliche deutliche Zeit- und Kosteneinsparungen, weil sie Fehler und Überarbeitungen ebenso wie die Verzögerungen, die durch IT-Besuche vor Ort entstehen, reduzieren.

75%

der fehlerhaften Prozesse können durch Automatisierung vermieden werden.

Automatisierte Änderungen kosten zudem 2% weniger, als wenn sie manuell durchgeführt werden.

Quelle: Gartner

2 Mehr Zeit für Strategiearbeit in der IT mit AIOps

Die manuelle Netzwerkkonfiguration ist nicht die einzige zeitaufwendige Tätigkeit. Die IT wendet fast 60% ihrer Zeit für die Behebung von Netzwerkproblemen auf[1].

Mit AIOps kann die IT Schwierigkeiten erkennen, bevor sie zu echten Problemen werden. In diesem Fall kann man KI und maschinelles Lernen einsetzen, um riesige Mengen an Metadaten, die in der Cloud gespeichert sind, auszuwerten und Rohdaten in eindeutige Erkenntnisse und Handlungsempfehlungen zu übersetzen.

Dynamische Basisdaten

Eine wichtige Funktion von AIOps ist die Fähigkeit, das grundlegende Netzwerkverhalten über längere Zeiträume hinweg dynamisch zu erfassen, wobei geänderte Bedingungen wie saisonale Muster im Datenverkehr automatisch berücksichtigt werden. Auf diese Weise muss die IT keine falsch-positiven Meldungen nachverfolgen, denn auch die Abstumpfung gegenüber Warnungen kann sich negativ auf die Ressourcen auswirken.

Dynamische Basisdaten sind auch deshalb von Vorteil, weil es für die IT zeitaufwendig ist, statische SLAs (Service Level Agreements) für jeden Standort manuell festzulegen und zu pflegen. Die IT kann das Netzwerkverhalten in Echtzeit überwachen und Schwierigkeiten somit sofort erkennen und darauf reagieren.

Fünf Vorteile von AIOps und Netzwerkautomatisierung

1. Optimierte Nutzererfahrung
2. Schnellere Netzwerkservicebereitstellung
3. Höhere Zuverlässigkeit des Netzwerks
4. Einheitliche Netzwerkkonfiguration
5. Schnellere Problembehebung

[1]*Quelle: EMA, Network Management Megatrends, 2020*

Erkennung von Anomalien

Mithilfe der Erkennung von Anomalien kann die IT Probleme automatisch identifizieren und mit ihrer Behebung beginnen – oft sogar noch bevor den Nutzern überhaupt auffällt, dass es ein Problem gibt. Noch besser: Mit den entsprechenden KI-gestützten Erkenntnissen kann die zugrunde liegende Ursache ermittelt werden. So weiß die IT genau, was sie wie beheben muss. Die Probleme werden außerdem anhand ihres Schweregrads in Kategorien eingeteilt, damit die IT Änderungs- und Verbesserungsmaßnahmen anhand ihrer geschäftlichen Auswirkungen priorisieren kann.

Branchen- oder Standortvergleiche

Und nicht zuletzt können in der Cloud verwaltete Netzwerke anonymisierte Branchenvergleiche aus einem gemeinsamen Datenbestand nutzen. Hier sind Informationen von Kunden mit ähnlichen Standort- oder Netzwerkcharakteristiken zusammengefasst, sodass die IT proaktiv Konfigurationsänderungen vornehmen kann, die letztendlich zu Leistungs- oder Kapazitätsverbesserungen gegenüber der vorhandenen Infrastruktur führen.

Wie können Netzwerke durch KI optimiert werden?

Ein Einzelhändler hatte Schwierigkeiten mit dem langsamen WLAN in allen seinen Filialen. Der IT fehlten jedoch die Daten oder Bezugspunkte, um das Problem richtig diagnostizieren und beheben zu können.

Mit **AIOps** konnte das Problem erkannt und validiert werden. Wenn Kunden, die die Filiale einmal besucht hatten, an dem Geschäft vorbeigingen, versuchten ihre Geräte, erneut eine Verbindung zum WLAN der Filiale herzustellen. Eine empfohlene Konfigurationsänderung konnte diesen unerwünschten Datenverkehr von Passanten zu 98% beseitigen und so zu einer verbesserten Leistung für legitime Nutzer beitragen.

Ergebnis: 25% mehr WLAN-Kapazität, ganz ohne neue Hardware.

3 Nutzererfahrung überall überwachen und verbessern

Menschen erwarten eine hervorragende Nutzererfahrung, wenn sie über Unternehmensnetzwerke auf Anwendungen oder andere digitale Dienste zugreifen. Es wird jedoch immer schwieriger, die Anwendungsleistung zu bewerten und zu verbessern, da die meisten IT-Überwachungstools die eigentliche Nutzererfahrung der Endbenutzer gar nicht berücksichtigen.

Dementsprechend wird ein Drittel (33%) der Netzwerk- oder Anwendungsprobleme von Endbenutzern gemeldet[1]. Das bedeutet, die IT kann im Umgang mit Problemen mit geschäftlichen Auswirkungen häufig nur reagieren. Dabei wird außerdem davon ausgegangen, dass die IT-Mitarbeiter vor Ort sind oder über einen geeigneten Remotezugriff verfügen, um das Problem überhaupt beheben zu können.

Eine einheitliche Infrastruktur mit einer in der Cloud verwalteten Netzwerklösung kann hier Abhilfe schaffen, weil sie der IT die Möglichkeit gibt, die Nutzer-, Geräte- und Anwendungsleistung von überall aus zu überwachen. Lösungen mit einer clientseitigen Überwachung, die das Nutzerverhalten nachahmen, liefern zusätzliche Informationen und helfen der IT, die Auswirkungen von Netzwerkänderungen auf Anwendungen und die Mitarbeiter oder Kunden, die versuchen, eine Verbindung damit herzustellen, zu beurteilen und zu validieren.

[1]*Quelle: EMA, Network Management Megatrends, 2020*

4 Unterstützung von Telearbeit bei geringerem IT-Aufwand

COVID-19 hat für eine nie da gewesene Zahl von Telearbeitern gesorgt. Die Arbeit im Homeoffice wird uns erhalten bleiben, da viele Mitarbeiter auch weiterhin zumindest teilweise Telearbeit machen werden. An hybriden Arbeitsplätzen greifen Mitarbeiter über unterschiedliche Netzwerke auf geschäftliche Anwendungen zu – mal unter der Kontrolle der IT, mal nicht. Wegen der unterschiedlichen Netzwerkbedingungen haben Telearbeiter in 70% der Unternehmen mehrmals die Woche Schwierigkeiten mit der IT-Leistung.

In der Cloud verwaltete Netzwerke tragen dazu bei, dass die Mitarbeiter überall arbeiten können, als wären sie im Büro. Solche Lösungen können sichere Konnektivität zu den Mitarbeitern nach Hause bringen, entweder über Remote Access Points oder über einen VPN-Dienst. Beide Optionen sollten für alle Mitarbeiter leicht zu installieren sein und einen zuverlässigen Zugriff auf Apps und Daten bieten – und dabei eine sichere Verbindung aufrechterhalten.

Die IT erhält vollständige Transparenz und Unterstützung bei der Fehlerbehebung über die Cloud, um sich um Probleme zu kümmern und sie zu beheben. Auf diese Weise kann die IT die Kosten für die Bearbeitung von Support-Tickets reduzieren und Arbeitsausfälle mit ihren exponentiellen Auswirkungen vermeiden.

TELEARBEIT BLEIBT UNS ERHALTEN

70%

der Unternehmen in den USA und der EU werden nach COVID-19 auf Hybridarbeit umstellen.

Quelle: Forrester, Mai 2021

5 Höhere Sicherheit für BYOD und IoT

Die Unterstützung von Telearbeitern mag zur neuen Normalität geworden sein, aber es wird immer Sicherheitsbedenken geben, wenn Mitarbeiter von außerhalb der herkömmlichen IT-Umgebung auf Unternehmensressourcen zugreifen. Gleichzeitig werden in den Büros immer mehr IoT-Geräte eingesetzt, die im Grunde nicht vertrauenswürdig sind. Wenn es dann auch noch an Transparenz mangelt, ist das Risiko noch größer.

Cloudbasierte Netzwerke können der IT helfen, Sicherheitsrichtlinien und genehmigte Zugriffsebenen für das Netzwerk zu erweitern und zu den Mitarbeitern – im Büro, unterwegs oder zu Hause – zu bringen. Auf Richtlinien basierende Automatisierung ersetzt statische Konzepte wie VLANs oder ACLs und Funktionen wie Intrusion Detection und Prevention verhindern, dass Bedrohungen aus SaaS-Anwendungen, die über das Internet bereitgestellt werden, hineingelangen können.

Im Hinblick auf die Transparenzlücken beim IoT sollten Sie über Lösungen nachdenken, die eine KI-basierte Geräteprofilierung ermöglichen, bei der alle Geräte im Netzwerk laufend identifiziert werden. Durch Nachverfolgen der Gerätenutzung und des Geräteverhaltens kann die IT sicherstellen, dass geeignete Richtlinien durchgesetzt werden.

IoT ERHÖHT DAS RISIKO

80%

der IT-Abteilungen haben IoT-Geräte im Netzwerk gefunden, die sie nicht installiert oder abgesichert haben.

Quelle: Gartner, Februar 2021

Endergebnis: Höhere Effizienz, niedrigere Gesamtbetriebskosten

In der Cloud verwaltete Netzwerke bieten eine wirkungsvolle Möglichkeit, operative Exzellenz für die IT-Infrastruktur und die Betriebsmannschaftenzu erreichen. Mit den folgenden vier Möglichkeiten können Unternehmen einen besseren ROI erzielen und die Gesamtbetriebskosten des Netzwerks reduzieren:

Einsparungen bei den Gesamtbetriebskosten

- Geringere Serverkosten (keine Heizung, Kühlung oder Wartung)
- Geringere Fahrtkosten (weniger Besuche vor Ort, niedrigere Reisekosten)
- Geringere Arbeitskosten (deutlich weniger Fehler und Überarbeitungen)

Verbesserte IT-Produktivität

- Einheitliche Verwaltung (keine manuelle Zuordnung, kein Wechsel von Tool zu Tool)
- KI-gestützter Betrieb (vereinfacht Fehlerbehebung und Aktualisierungen)
- Automatisierte Software-Updates (kürzere Wartungszeitfenster)

Höhere IT-Agilität

- Einfache Bereitstellung von Netzwerken auf dem Campus und in den Zweigstellen
- Einfache Aktivierung neuer Funktionen
- Keine Herausforderungen bei Servern und Größenanpassung

Bessere Resilienz

- Höhere Skalierbarkeit (Mikroservice-Architektur und Web-Scale-Design)
- Höhere Verfügbarkeit (global in Rechenzentren von Cloud-Anbietern gehostet)

aruba
a Hewlett Packard Enterprise company

Sichere Netzwerke sind die Mission von Aruba

Mit Aruba ESP und seiner wachsenden Palette an Unfied-Infrastructure-Lösungen können Unternehmen, die Effizienz und Agilität der IT optimieren und es ihren Teams ermöglichen, den wachsenden Anforderungen und Schwierigkeiten von global agierenden Unternehmen zu begegnen.