2595

NET

1-2/2023

Zeitschrift für Kommunikationsmanagement

Blick über den Tellerrand

Technikalternativen für sichere Firmennetze

Metaverse

Reif für Breitenanwendungen

NET Verlag und Zeitschrift GbR, Löwenberger Weg 14, 16766 Kremmen
Postvertriebsstück, Entgelt bezahlt

In Zusammenarbeit mit

BREKO
Bundesverband Breitbandkommunikation e.V.

Controlware Network Day

„Wir müssen das Thema Netzwerk fundamental neu denken“

Intelligente, cloudgesteuerte Netzwerke arbeiten leistungsfähiger, sicherer und wesentlich agiler. Die Cloud ist das Fundament für eine nachhaltige Automatisierung des Netzwerkbetriebes (Foto: Gerd Altmann, pixabay)

Bernhard Reiman

Die hybriden Arbeitsmodelle des New Normal stellen neue Anforderungen an die Enterprise Networks der Unternehmen. Auf dem Controlware Network Day sprachen Olaf Hagemann, Director of Systems Engineering DACH bei Extreme Networks, und Controlware CEO Bernd Schwefing über die neuesten Entwicklungen rund um das Networking.

NET: Der Wechsel zwischen Büro und Homeoffice gehört heute in vielen Unternehmen zum guten Ton, und auch sonst geht das hybride „New Normal“ der Post-Covid-Ära mit einer Reihe tiefgreifender Veränderungen einher. Was bedeutet das für die Anforderungen an moderne Enterprise Networks?

Olaf Hagemann: Die Pandemie hat die Art, wie und wo wir arbeiten, radikal verändert. Viele Unternehmen waren zunächst skeptisch, ob die Öffnung der Netzwerke für hunderte von Homeoffices eine angemessene Antwort auf die Krise ist – letztlich erwies sich dieser Schritt aber als unumgänglich, um weiter produktiv arbeiten zu können. Und gemeinsam haben wir einen Weg gefunden, ein erfolgreiches hybrides Arbeiten zu ermöglichen. Der Preis dafür war allerdings hoch: Die Perimeter rund um die Unternehmen haben sich endgültig aufgelöst, und diese Entwicklung wird sich auch nicht umkehren lassen. Es gilt jetzt also, die ad-hoc umgesetzten Schutzmaßnahmen schnellstmöglich in robuste und zukunftsfähige Netzwerkarchitekturen zu überführen.

NET: Was bedeutet das konkret – welche Anforderungen müssen die Unternehmen im Blick behalten?

Bernd Schwefing: Da gibt es eine ganze Reihe von Faktoren zu berücksichtigen.

Bernhard Reiman ist Objektleiter bei der NET

Die meisten unserer Kunden rücken bei ihren Modernisierungsvorhaben Aspekte wie Agilität, Stabilität, Effizienz, Sicherheit und – immer öfter – Nachhaltigkeit in den Fokus. Dabei setzt natürlich jedes Unternehmen eigene Schwerpunkte, die aus seinen individuellen Anforderungen resultieren, unter anderem der Verteilung der Standorte, der Cloud-Nutzung und der Latenz-Anforderungen produktionsnaher Applikationen. Nur zwei Aspekte sind allen gemeinsam: Sicherheit und ein möglichst einfaches Management. All dies müssen wir als IT-Dienstleister mit unseren Lösungen abbilden können, und dies, ohne dass die Komplexität der Technologie-Stacks weiter aus dem Ruder läuft.

NET: Die Komplexität des Tech-Stacks ist seit Jahren ein Thema, das die IT über alle Unternehmensgrößen und Branchen hinweg beschäftigt. Wie komplex sind moderne Enterprise-Netzwerke denn wirklich, Herr Hagemann?

O. Hagemann: In der Regel zu komplex. Seit Jahren integrieren Unternehmen immer neue Komponenten und Dienste, um von neuen Features zu profitieren. Dabei unterschätzen sie aber oftmals den enormen Managementaufwand, der mit dieser Expansion einhergeht. Den Tech-Stack ohne funktionelle Abstriche wieder beherrschbar zu machen, ist eine der dringlichsten Aufgaben der IT. Um es einmal an einem praktischen Beispiel festzumachen: In modernen Produktionsumgebungen verfügt heute jeder Akkuschrauber über eine eigene WLAN-Adresse. Dafür gibt es gute Gründe: Nur so lässt sich in Echtzeit tracken, wann das Gerät wofür verwendet wurde und wann es vorausschauend gewartet werden muss, um die Lebensdauer zu optimieren. Diese Netzwerkfähigkeit darf aber nicht bedeuten, dass jeder Akkuschrauber von der IT separat administriert, gepatcht und aktualisiert werden muss – wie es heute vielfach der Fall ist. Wenn wir die Komplexität reduzieren wollen, ohne den Leistungsumfang einzuschränken, müssen wir das Thema Netzwerk fundamental neu denken.

NET: Verfügen die Unternehmen jetzt, in einer wirtschaftlich angespannten Situation, denn überhaupt über die Ressourcen, um solche ambitionierten Projekte zu realisieren?

Olaf Hagemann

Wenn wir die Komplexität in industriellen Prozessen reduzieren wollen, ohne den Leistungsumfang einzuschränken, müssen wir das Thema Netzwerk fundamental neu denken

B. Schwefing: Da sprechen Sie einen wunden Punkt an. Die Modernisierung des Enterprise Networks fordert Unternehmen sowohl finanziell als auch personell viel ab. Unsere Erfahrung zeigt dabei, dass die Budgets oft die leichter lösbare Herausforderung darstellen. Die fehlenden Fachkräfte hingegen sind ein strukturelles Problem: Schon heute reichen die Personalressourcen kaum aus, um den Status quo zu erhalten, von ehrgeizigen Modernisierungsvorhaben ganz zu schweigen. Nicht umsonst zielen die genannten Kundenanforderungen – Agilität, Resilienz, Effizienz – letzten Endes alle darauf ab, das Team zu entlasten und neue Freiräume zu schaffen. Und das ist auch dringend notwendig, da sich die Lage weiter zuspitzen wird. 2030 soll es allein in Deutschland 1 Mio. offener IT-Stellen geben. Um also auf Ihre Frage zurückzukommen: Nein, nur mit den internen Teams wird sich die anstehende Modernisierungswelle kaum realisieren lassen. Aber mit den richtigen Partnern und den richtigen Technologien können Unternehmen heute die Weichen für ein zukunftssicheres, weitgehend automatisiertes und smartes Networking stellen.

NET: Und wie könnten diese Zukunftsmodelle aussehen, Herr Hagemann?

O. Hagemann: Noch vor drei oder vier Jahren haben sich die meisten Unternehmen auf sehr klassische Infrastrukturen verlassen, in denen die Benutzer – die Mitarbeiter – jeden Morgen zum Netzwerk kamen. Heute setzen sich immer mehr intelligente, dezentrale cloudbasierte Lösungen durch. Diese erkennen automatisch, wer sich wann und wo mit welchem Device anmeldet, und können die Nutzer optimal bei ihrer Arbeit unterstützen. Zum Beispiel, indem die wichtigsten Anwendungen besonders leistungsfähig bereitgestellt werden oder indem kritische Sicherheits-Features für einen zuverlässigen Schutz schon am Edge implementiert werden. Wir nennen dieses Konzept „Infinite Enterprise“: ein grenzenloses, skalierbares und softwaregesteuertes Netzwerk, das die Möglichkeiten der Cloud nutzt und dabei ganz auf die Anforderungen des einzelnen Benutzers zugeschnitten ist.

NET: Sind die deutschen Unternehmen bereit für ein solches cloudbasiertes Netzwerkkonzept, Herr Schwefing?

B. Schwefing: Durchaus. Die IT- und die Business-Verantwortlichen wissen um die immensen Vorteile, die ihnen cloudbasierte Technologien bieten – und konzentrieren sich jetzt darauf, diese Benefits sicher und compliancekonform

zu erschließen. Intelligente, cloudgesteuerte Netzwerke arbeiten leistungsfähiger, sicherer und wesentlich agiler. Und was mit Blick auf den angesprochenen Fachkräftemangel besonders wichtig ist: Die Cloud ist auch das Fundament für eine nachhaltige Automatisierung des Netzwerkbetriebes. Eine wesentliche Voraussetzung ist dabei, dass der Anbieter neben der Erfüllung der GDPR auch sicherstellt, dass die Unternehmen Transparenz und Steuerungsmöglichkeiten über die Daten haben, die in der Cloud verarbeitet werden.

NET: Ohne Cloud ist das Infinite Enterprise also undenkbar?

O. Hagemann: Ja. Die Cloud übernimmt bei uns nicht nur die Rolle des zentralen SDN-Controllers, sondern steuert als Data Lake auch die Machine Learning- und KI-Features bei. Dort steckt also die gesamte Intelligenz und damit auch der Mehrwert der Lösung. Vielleicht auch hier ein Beispiel aus der Praxis: Wenn uns ein japanischer Kunde signalisiert, dass es Kompatibilitätsprobleme zwischen zwei seiner Netzwerkkarten gibt und eine davon neu konfiguriert werden muss, erfahren dies automatisch auch alle deutschen Kunden, die diese Komponenten einsetzen – in Echtzeit, mit einer detaillierten Update-Anleitung. Das ist ein Riesenmehrwert, den man mit einer lokalen Lösung nie bieten könnte. Wie genau die Cloud eingebunden wird, entscheidet dabei der Kunde: Wir unterstützen völlig agnostisch alle großen Public Clouds sowie Private Clouds für besonders kritische Kunden. Eine dritte Alternative sind Distributed Clouds auf Kubernetes-Clustern, die dann von unseren Partnern und Providern gehostet werden.

NET: Wenn die Netzwerke über Software steuerbar werden, eröffnet das auch für Dienstleister und MSPs neue Möglichkeiten. Wo sehen Sie die Rolle von Controlware in diesem Szenario, Herr Schwefing?

B. Schwefing: Für uns ist das natürlich eine sehr spannende Konstellation, weil wir die gemeinsamen Kunden auf diese Weise in allen Phasen ihrer Netzwerkprojekte unterstützen können: vom Lösungsdesign über die Umsetzung bis hin zu individuell zugeschnittenen Managed Services. Diese umfassen sowohl das selektive Outtasking einzelner Bereiche als auch die Übergabe des kompletten Netzwerkbetriebes inklusive der Sicherheitsinfrastruktur an unsere Experten. Ergänzend dazu bieten wir überdies ein komplettes Portfolio von Cyber Defense Services an.

NET: Apropos Cyber Defense: Was unternimmt Extreme Networks, um die Daten der Kunden in der Cloud zu schützen?

O. Hagemann: Nun, zunächst einmal ist es wichtig festzuhalten, dass die Daten, die wir erfassen und mit denen wir arbeiten, in aller Regel nicht hochgradig sensibel sind. Beim einem Großteil handelt es sich um Netzwerkdaten, globale IP-Adressen und ähnliches. Trotzdem gehen wir natürlich sehr sorgsam mit diesen Daten um: Unsere Rechenzentren werden strengsten Sicherheitsstandards gerecht und im Falle deutscher Kunden werden deren Daten auch ausschließlich in Deutschland gehostet. Zudem sind sie auch nicht von extern erreichbar. Perspektivisch werden wir schon bald noch einen weiteren wichtigen Schritt gehen und eine durchgängige Zero-Trust-Architektur implementieren. Konkret heißt das: Wir werden jede Anwendung über einen eigenen verschlüsselten Tunnel übertragen – und über leistungsfähige Hyper- und Micro-Segmentierung in der Lage sein, kompromittierte Devices zuverlässig zu isolieren.

Bernd Schwefing

Mit den richtigen Partnern und den richtigen Technologien können Unternehmen heute die Weichen für ein zukunftssicheres, weitgehend automatisiertes und smartes Networking stellen

NET: Als ausgemachter Security-Spezialist hat Controlware das Thema Zero Trust sicher auch auf dem Schirm, und fasst es wahrscheinlich sogar noch weiter, richtig?

B. Schwefing: Vereinfachend gesagt, trägt das Konzept „Zero Trust" der Tatsache Rechnung, dass in den beschriebenen modernen Infrastrukturen – mit ihren flexiblen Arbeitsplätzen und der Integration von Cloud-Ressourcen verschiedener Anbieter – ein reiner Perimeter-Schutz, der einen sicheren Bereich von der Außenwelt trennt, schon länger nicht mehr ausreicht. Stattdessen muss an jeder Stelle erneut kontrolliert werden. Aus Netzwerkperspektive bedeutet dies, die kritischen Bereiche zu identifizieren und zu bewerten, die Verkehrsflüsse im Netz sichtbar zu machen und auf dieser Basis Segmentierungs-Policies zu erstellen und umzusetzen. Mit Blick auf die Komplexität heutiger Infrastrukturen ist das allerdings kein einmaliger Vorgang. Der Prozess muss laufend überwacht und angepasst werden – und das kann nur auf Basis automatisierter Abläufe funktionieren.

Herr Hagemann, Herr Schwefing, wir danken Ihnen für das Gespräch.

www.controlware.de