RESEARCH
Influence and insight
through social media

Oktober 2016

Wettbewerbsvorteile erzielen durch

LEISTUNGSSTARKEN NETZWERKÜBERGANG

WHITEPAPER

Erstellt von
Zeus Kerravala

ZK Research
A Division of
Kerravala Consulting

INFORMATIONEN ZUM VERFASSER

Zeus Kerravala ist Gründer und Principal Analyst von ZK Research. Kerravala bietet seinen Kunden taktische Beratungsleistungen und strategische Unterstützung, um ihren Erfolg sowohl im derzeitigen Wirtschaftsklima als auch langfristig zu sichern. Seine Forschungs- und Beratungsleistungen stehen folgenden Kundenkreisen zur Verfügung: Endbenutzer-IT- und Netzwerkmanagern; Anbietern von IT-Hardware, -Software und -Services sowie Mitgliedern der Finanzbranche, die in die von ihm beratenen Unternehmen investieren möchten.

EINFÜHRUNG: UNTERNEHMEN SIND HEUTE NETZWERKORIENTIERT

Die Digitalisierung verändert die Geschäftswelt schneller als je zuvor. Unternehmen, die sich der Digitalisierung bereits verschrieben haben, übernahmen auf ihren jeweiligen Märkten schnell Führungspositionen, während alle anderen weiter zurückgefallen sind. Umfragen von ZK Research zufolge sind digitale Unternehmen um 64 Prozent rentabler als andere, die diesen Wechsel nicht vollzogen haben. Aus diesem Grund ist die Digitalisierung eine wichtige Initiative für IT-Verantwortliche und Führungskräfte.

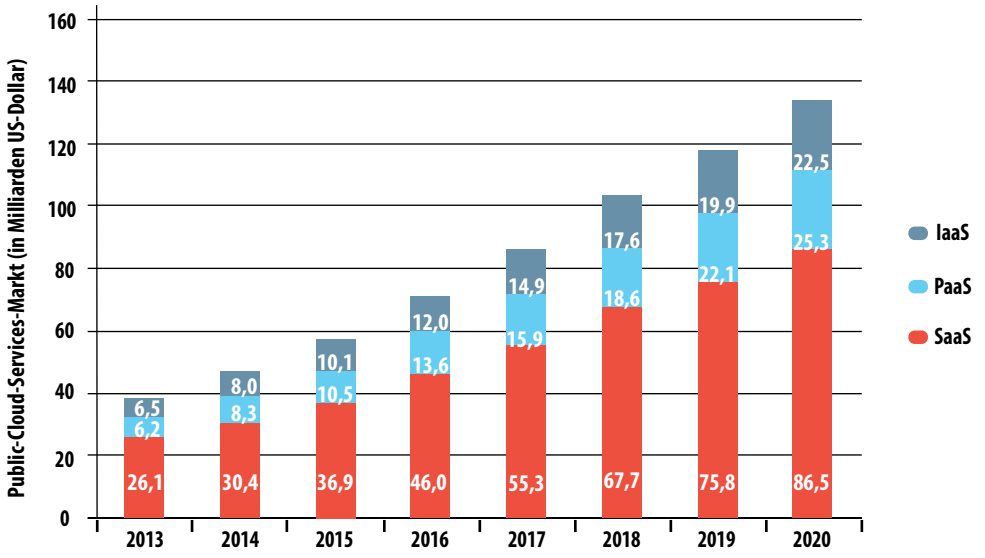
Wie bereits andere größere Veränderungen zuvor erfordert auch der digitale Wandel den Einsatz neuer Technologien. Die letzte bedeutende geschäftliche Veränderung – das Zeitalter des Internets – wurde durch das Zusammenspiel aus kostengünstigem PC-Computing, dem Betriebssystem Windows, der Entwicklung des Browsers und der zunehmenden privaten Breitband-Nutzung beschleunigt.

Das digitale Zeitalter wird durch zahlreiche neue Technologien wie Cloud-Computing, Mobilität, dem Internet of Things (IoT), Big Data und Collaboration geprägt sein. All diese Technologien mögen zwar wie einzelne Komponenten ohne Bezug zueinander erscheinen, haben aber eine besondere Gemeinsamkeit: Sie sind alle netzwerkorientiert, d. h. das Netzwerk spielt für eine erfolgreiche Bereitstellung eine zentrale Rolle. So steigt beispielsweise die Nutzung von Cloud-Services explosionsartig an (Abbildung 1); Voraussetzung für benutzerfreundliche Cloud-Services sind jedoch qualitativ hochwertige Netzwerkservices.

In den vergangenen Jahren haben viele Experten prognostiziert, das Netzwerk würde zur Massenware werden. In diesem Szenario wäre die beste Lösung der Kauf des kostengünstigsten Produkts, da es zwischen den Anbietern ansonsten nur sehr wenige Unterschiede gäbe. Dieser Trend hat sich in anderen Bereichen der IT wie dem persönlichen Computing bewahrheitet, weshalb spekuliert wurde, dass die Netzwerkbranche dieselbe Richtung einschlagen würde.

Richtig ist, dass handelsübliche Switches kostengünstiger als modernste und häufig hochpreisige Switches sind. Die Kosten eines Switches sollten jedoch nicht

Abbildung 1: Zunehmende Nutzung von Cloud-Services



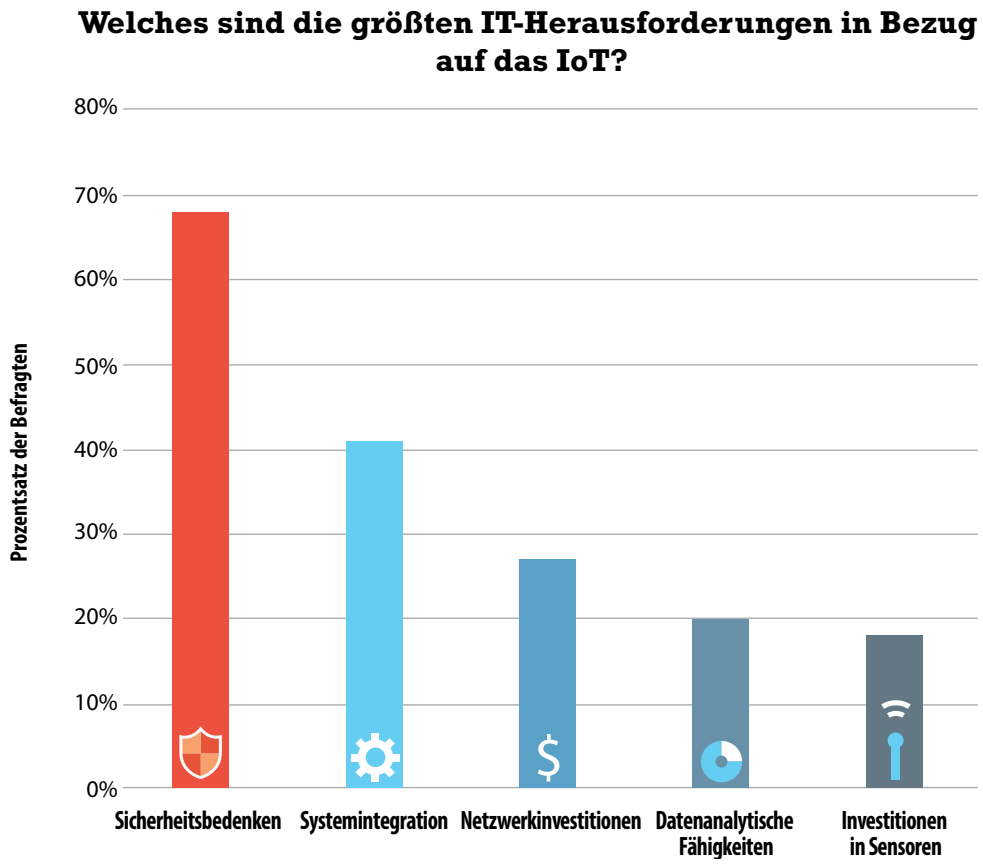
ZK Research: Global Cloud Forecast 2016

allein anhand des Gerätepreises beurteilt werden. ZK Research vertritt vielmehr den Standpunkt, dass ein handelsüblicher Switch langfristig höhere Kosten verursachen wird, und zwar aus den folgenden Gründen:

Sicherheitsrisiken: Das Netzwerk bietet Zugriff auf alle wertvollen Daten eines Unternehmens. Wenn keine geeigneten Vorsichtsmaßnahmen getroffen wurden, besteht hier ein hohes Risiko durch Hackerangriffe. Jedes mit dem Netzwerk verbundene Gerät ist heute angreifbar. Bisher haben Sicherheitsteams auf unternehmenseigenen PCs Agents zum Schutz der Endpunkte installiert. Heute muss die IT die zunehmende Nutzung privater Mobilgeräte und IoT-Endpunkte berücksichtigen, die sich mit Agents wesentlich schwieriger schützen lassen. IoT-Geräte stellen eine große Herausforderung dar, da die meisten IoT-Endpunkte keine Möglichkeit zur Ausführung von Agents bieten. Darüber hinaus konnten laut IoT Survey 2016 von ZK Research 78 Prozent der befragten IT-Mitarbeiter nicht sicher angeben, ob IoT-Geräte mit dem Netzwerk verbunden waren. Aus diesem Grund zählt die Sicherheit zu den wichtigsten Aspekten bei der IoT-Bereitstellung (Abbildung 2).

Kosten durch Ausfallzeiten: Handelsübliche Switches werden im Allgemeinen kostengünstiger hergestellt als Premium-Switches und bieten

Abbildung 2: Anliegen bei der IoT-Bereitstellung



ZK Research: Network Purchase Intention Study 2016

IT-Verantwortliche müssen den Netzwerkübergang als strategische Ressource betrachten. Die Wahl sollte auf einen Anbieter fallen, der vor allem Innovationen fördert und nicht nur die Kosten senkt.

keine vergleichbare Ausfallsicherheit. Das digitale Zeitalter ist geprägt durch umfassende Vernetzung; Ausfallzeiten kosten Unternehmen bares Geld. ZK Research beziffert die durchschnittlichen Kosten durch Ausfallzeiten in allen Branchen auf etwa 1,7 Millionen US-Dollar pro Stunde. Schon kleine Abweichungen bei der Betriebszeit können sämtliche Einsparungen durch den Einsatz eines handelsüblichen Switches schnell zunichtemachen.

Kosten durch mangelnde Benutzerfreundlichkeit: Unternehmen geben enorm hohe Summen für neue Technologien zur Steigerung der Benutzerproduktivität aus. ZK Research hat errechnet, dass Benutzer aufgrund schlechter Anwendungsleistung im Durchschnitt 14 Prozent weniger produktiv sind. Ein handelsüblicher Switch kann bei hoher Belastung keine vergleichbare Leistung erzielen, was sich direkt auf die Benutzerproduktivität auswirkt.

Kosten durch fehlende Geschäftsmöglichkeiten: Die Digitalisierung ist kein einmaliges Ereignis. Unternehmen müssen kontinuierlich Daten erfassen und analysieren, um neue Erkenntnisse gewinnen und sich gegenüber Mitbewerbern behaupten zu können. Der Netzwerkübergang kann zahlreiche Daten über Benutzer, Geräte und Anwendungen sowie andere kontextbezogene Informationen liefern. Handelsübliche Netzwerkgeräte bieten keine vergleichbare Instrumentierung und Transparenz, um dem Unternehmen relevante Erkenntnisse liefern zu können.

Ein Netzwerk aus handelsüblichen Komponenten wird zudem auf lange Sicht Innovationen ausbremsen. Hersteller von Netzwerkprodukten verwenden die kostengünstigsten vorgefertigten Komponenten und senken damit die Engineering-Kosten. Wären alle Produkte identisch, bestünde theoretisch der einzige Wettbewerbsvorteil im Preis, was aber das Innovationspotenzial minimieren würde.

Allerdings hat sich diese These als falsch erwiesen: Mehr als je zuvor kommt es heute auf die Wahl des passenden Netzwerks an – insbesondere am Netzübergang, dem Verbindungspunkt für Benutzer, Anwendungen und Geräte. IT-Verantwortliche müssen den Netzwerkübergang als strategische Ressource betrachten. Die Wahl sollte auf einen Anbieter fallen, der vor allem Innovationen fördert und nicht nur die Kosten senkt

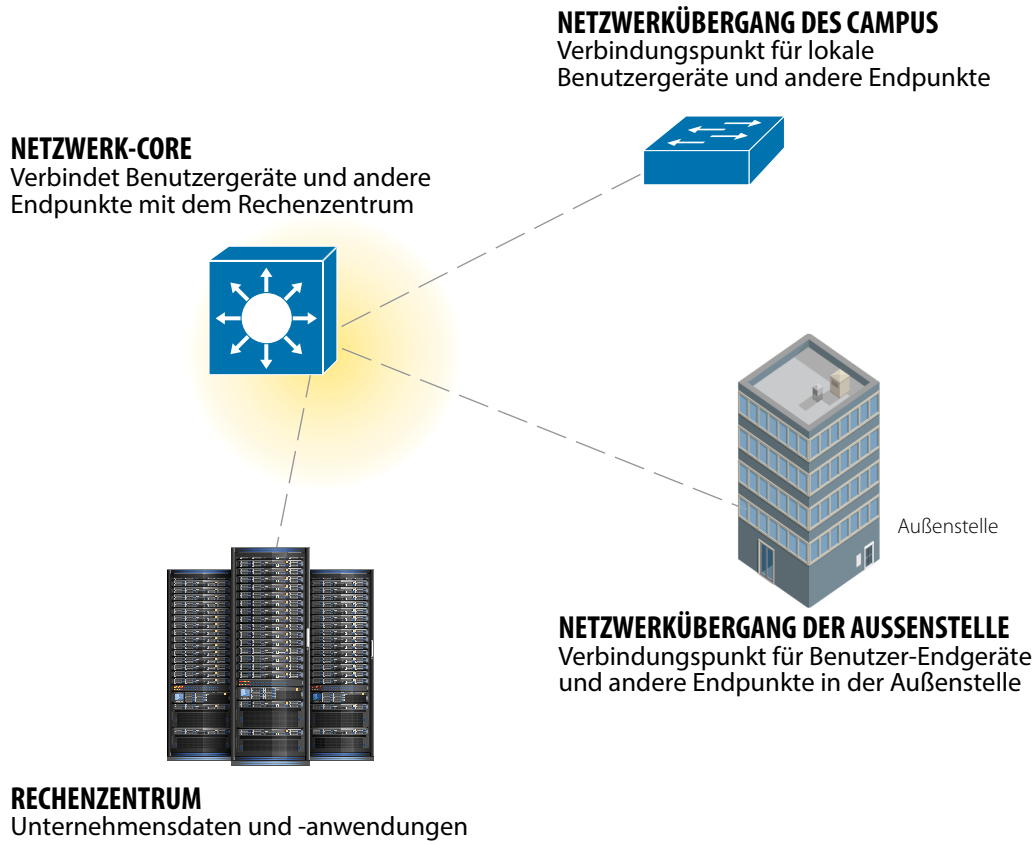
ABSCHNITT II: DIE ROLLE DES NETZWERKÜBERGANGS

Fachfremde Techniker haben häufig Schwierigkeiten, die Funktionsweise von Netzwerken zu verstehen. Ein Netzwerk mag zwar wie eine Einzelkomponente funktionieren, besteht aber tatsächlich aus mehreren Ebenen oder Schichten mit bestimmten Funktionen (Abbildung 3).

Das Rechenzentrum und der Netzwerk-Core sind dabei besonders wichtig. Ihre Hauptfunktion besteht darin, den Datenverkehr schnellstmöglich von einem Ort zum anderen zu transportieren. Noch vor zehn Jahren waren am Netzwerkübergang hauptsächlich PCs und Drucker mit dem Unternehmensnetzwerk verbunden. Im Zuge der Digitalisierung ist der Netzwerkübergang, bestehend aus Campus- und Außenstellen-Netzwerkübergang, jedoch immer wichtiger geworden. Nachfolgend sind alle Funktionen aufgeführt, die heute vom Netzwerkübergang erfüllt werden:

Erster Durchsetzungspunkt für Sicherheitsfunktionen: Laut Security Survey 2016 von ZK Research treten 80 Prozent der Sicherheitsverletzungen innerhalb des Netzwerkperimeters auf. Dies hat erhebliche Auswirkungen auf die Sicherheitsstrategie, da die Unternehmens-Firewall keinen Schutz vor Sicherheitsbedrohungen bietet. Der Netzwerkübergang ist der ideale Ort zur Anwendung und Validierung von Richtlinien, da auf diese Weise der

Abbildung 3: Die Rolle der Netzwerkebenen



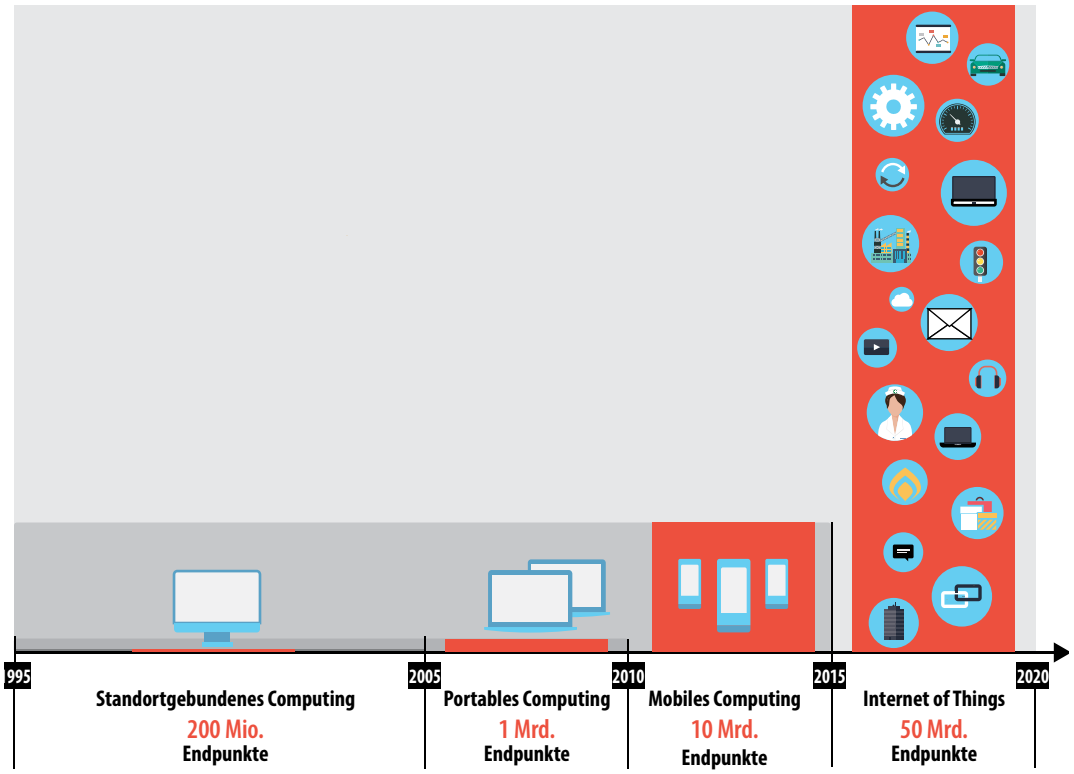
ZK Research, 2016

Benutzerzugriff auf erforderliche Ressourcen nicht eingeschränkt wird. Mittels am Netzwerkübergang festgelegter Sicherheitsrichtlinien können die meisten internen Bedrohungen abgewehrt und im Fall einer Sicherheitsverletzung ihre weitere Ausbreitung verhindert werden.

Grundlage für das IoT: ZK Research schätzt, dass die Anzahl der vernetzten Endpunkte bis 2020 rasant ansteigen wird (Abbildung 4). Da IoT-Verbindungen über IP erfolgen, werden Geräte wie Gesundheitssysteme und LED-Beleuchtungssysteme am Netzwerkübergang angebunden. Neben der Vernetzung werden viele dieser Geräte außerdem per Power over Ethernet (PoE) über das Netzwerk mit Strom versorgt. Wenn die erforderlichen Funktionen nicht am Netzwerkübergang vorhanden sind, können Unternehmen ihre IoT-Investitionen nicht optimal nutzen.

Optimierung der Anwendungsleistung: Alle Geschäftsanwendungen müssen den Netzwerkübergang durchlaufen – unabhängig davon, ob sie sich im Rechenzentrum des Unternehmens oder in der Cloud befinden. Am Netzwerkübergang erfolgt auch die Priorisierung von Anwendungen, wodurch Beeinträchtigungen von Echtzeit- oder geschäftskritischen Anwendungen verhindert werden.

Abbildung 4: Mehrere Milliarden Verbindungen am Netzwerkübergang durch das IoT



ZK Research, 2016

Verbessertes Kundenerlebnis: Eine der wichtigsten Initiativen bei der Digitalisierung für Unternehmen ist ein differenziertes Kundenerlebnis. Digitale Technologie kann die Art und Weise verändern, wie Kunden einkaufen, Studenten lernen und Ärzte praktizieren. Eine mangelnde Leistung am Netzwerkübergang kann jedoch kundenseitige Services erheblich beeinflussen, wodurch die Kundentreue stark gefährdet ist. Einer aktuellen Umfrage von ZK Research zufolge haben zwei Drittel der Millennials in den letzten 12 Monaten aufgrund eines schlechten Anwendererlebnisses ihren Anbieter gewechselt.

Höherer geschäftlicher Wert: Mit dem Netzwerkübergang können neue Erkenntnisse über die Entwicklung des Unternehmens gewonnen werden. Sämtlicher Datenverkehr durchläuft den Netzwerkübergang und kann somit mühelos vom Unternehmen erfasst und analysiert werden. Anhand von Informationen über Benutzer, Geräte, Anwendungen und Bedrohungen können fundierte Entscheidungen schneller als bei Mitbewerbern getroffen werden. So kann das Unternehmen eine nachhaltige Führungsposition einnehmen.

ABSCHNITT III: WICHTIGE FRAGEN FÜR DEN AUFBAU EINES LEISTUNGSSTARKEN NETZWERKÜBERGANGS

Bei der Wahl eines Netzwerkanbieters gibt es zahlreiche Optionen: von kostengünstigen handelsüblichen Produkten bis zu höherwertigen Produkten mit vollständigem Funktionsumfang. Eine Evaluierung dieser Produkte kann sich

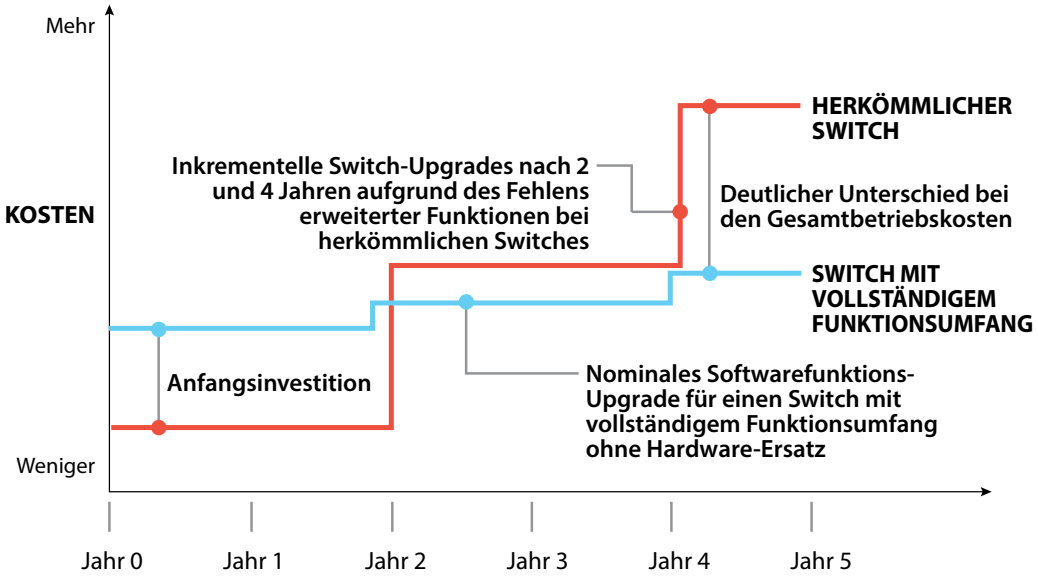
aufgrund der großen Unterschiede bei Preis, Funktionsumfang, Verwaltbarkeit und Sicherheitsaspekten jedoch schwierig gestalten. Nachfolgend sind die wichtigsten Fragen aufgeführt, die in Unternehmen beim Aufbau eines leistungsstarken Netzwerkübergangs gestellt werden sollten.

Wie hoch sind die Gesamtbetriebskosten über einen Zeitraum von fünf Jahren?

Angesichts des zunehmenden Einsatzes digitaler Technologien sollte das Unternehmensnetzwerk als digitale Grundlage betrachtet werden. Bei richtiger Implementierung können Netzwerke umfassende Services für den Netzwerkübergang bereitstellen. Dabei dürfen jedoch die Möglichkeit einer mühelosen Anpassung an ein wechselndes Geschäftsumfeld und die Unterstützung integrierter erweiterter Funktionen ohne Unterbrechung der Betriebsabläufe nicht außer Acht gelassen werden. Nur so können die Gesamtbetriebskosten langfristig deutlich reduziert werden.

Bei der Evaluierung von Produkten am Netzwerkübergang sollten Unternehmen zur Berechnung der Gesamtbetriebskosten mindestens die nächsten fünf Jahre (entspricht ungefähr einem Austauschzyklus) berücksichtigen. Wie Abbildung 5 zeigt, liegen die Gesamtbetriebskosten handelsüblicher Produkte zu Beginn des Lebenszyklus scheinbar deutlich niedriger. Da Unternehmen jedoch immer wieder neue Services benötigen und inkrementelle Upgrades durchführen müssen, können die Gesamtbetriebskosten eines handelsüblichen Switches schnell rasant ansteigen, weil er häufiger ersetzt werden muss. Darüber hinaus kann die Wahl der falschen langfristigen Produkte zu unnötigen Ausfallzeiten, entgangenen Geschäftsmöglichkeiten und einer inkonsistenten Verwaltbarkeit der Geräte führen. Ein CTO beschrieb einen Switch mit vollständigem Funktionsumfang gegenüber ZK Research als Schweizer Messer: Er war zwar nicht sicher, wann er all diese Funktionen benötigen würde, wusste aber, dass er bei Bedarf unmittelbar darauf zurückgreifen konnte.

Abbildung 5: Netzwerk-Switches mit vollständigem Funktionsumfang bieten erheblich niedrigere Gesamtbetriebskosten als handelsübliche Produkte



ZK Research, 2016

Der digitale Wandel bringt fortlaufende Veränderungen mit sich. Daher ist es wichtig, das Innovationspotenzial des Netzwerks zu kennen.

Der digitale Wandel bringt fortlaufende Veränderungen mit sich. Daher ist es wichtig, das Innovationspotenzial des Netzwerks zu kennen – unabhängig davon, ob es sich um eine vollständig neue Bereitstellung oder die Aktualisierung eines bestehenden Netzwerks handelt. Die Frage kann in drei Hauptkategorien unterteilt werden: Innovationen, Sicherheit und Flexibilität.

Wie fördert das Netzwerk Innovationen?

Das Netzwerk stellt nicht nur Verbindungen zur Verfügung, sondern muss auch digitale Aktivitäten ermöglichen. Dadurch stellen sich hinsichtlich der Innovation folgende Fragen:

1. **Kann die Lösung Verfügbarkeit und konsistente Servicebereitstellung gewährleisten?** Die Zeiten folgenschwerer Netzwerkausfälle sind vorbei. Die Aufrechterhaltung des Netzwerkbetriebs ist relativ einfach; schwieriger ist es dagegen, beim Ausfall einer Netzwerkkomponente eine Beeinträchtigung des Anwendererlebnisses zu vermeiden. Netzwerke müssen sich heute automatisch an solche Ausfälle anpassen und dabei eine unveränderte empfundene Leistung gewährleisten. Die IT muss außerdem über Anomalien und Trends im Netzwerk informiert werden, um deren potenzielle Auswirkungen zu erkennen. Mithilfe von Telemetriedaten können Anwendungsprobleme rasch lokalisiert und behoben werden. Laut Wi-Fi Operations Survey 2016 von ZK Research verbringen fast 50 Prozent der Befragten mindestens 25 Prozent ihrer Zeit mit der Behebung von Wi-Fi-Problemen. Unternehmen benötigen Methoden, um diesen Zeitaufwand deutlich zu reduzieren.

2. **Kann sich die Lösung schnell an neue und unerwartete Anforderungen anpassen?** Die Netzwerkanforderungen können sich in Sekundenschnelle ändern. Daher müssen Unternehmen unbedingt eine Lösung bereitstellen, die Wi-Fi-Netzwerke automatisch an die Skalierung von Clients und an eine veränderte Signalqualität anpassen kann.

3. **Kann die Lösung die Leistung und Akkulaufzeiten von Geräten verbessern?** Benutzer greifen hauptsächlich über Mobilgeräte auf Informationen zu. Das Netzwerk muss automatisch die verbundenen Geräte erkennen und geeignete Anpassungen vornehmen, um in der neuen mobilen Welt ein optimales Anwendererlebnis bieten zu können. Durch optimiertes Roaming können Akkulaufzeiten verbessert und Benutzer unterwegs besser vernetzt werden.

4. **Kann das Netzwerk präzise Erkenntnisse über interne und externe Elemente liefern?** Daten sind der Schlüssel. Das Netzwerk ist eine wertvolle Quelle von Informationen über Benutzer, Geräte, Anwendungen und sogar Bedrohungen. Der Wert dieser Daten ist jedoch direkt von ihrer Genauigkeit abhängig – und die Genauigkeit entspricht der Granularität. Eine präzise Ansicht mit sehr vielen Datenpunkten liefert realistischere Erkenntnisse als eine gröbere Ansicht mit nur regelmäßigen Datenpunkten. Durch erweiterte Netzwerkservices wie die vollständige Triangulation von Clients, Netzwerken oder Anwendungen können neue Anwendungsfälle und Kundenerlebnisse geschaffen werden. Mithilfe dieser Informationen kann die IT verwertbare, unternehmensrelevante Daten bereitstellen und sich so mehr Gehör verschaffen.

Digitale Unternehmen benötigen eine flexible IT-Grundlage, um schneller als ihre Mitbewerber auf die Marktdynamik reagieren zu können.

5. Kann die Lösung neue IoT-Geräte unterstützen, die nicht ständig von einem Benutzer bedient werden? Der Netzwerkübergang kann die Verfügbarkeit eines Endpunkts verbessern. Viele Geräte wie etwa IoT-Komponenten sind über eine PoE-Schnittstelle (Power over Ethernet) mit dem Netzwerk verbunden, sodass bei Ausfall des Switches ein Single Point of Failure entsteht. Die Switches, mit denen diese Geräte verbunden sind, müssen über Ausfallsicherheitsfunktionen verfügen, um Ausfallzeiten zu minimieren. Da außerdem immer mehr Geräte über Switches mit Strom versorgt werden, muss der Switch eine ausreichende Leistung bereitstellen.

Ist das Netzwerk flexibel genug für das digitale Zeitalter?

Digitale Unternehmen benötigen eine flexible IT-Grundlage, um schneller als ihre Mitbewerber auf die Marktdynamik reagieren zu können. Die IT ist jedoch immer nur so flexibel wie die am wenigsten dynamische Komponente – in vielen Fällen das Netzwerk. Der Netzwerkübergang muss ebenso flexibel wie die übrigen Komponenten sein, ohne jedoch höhere Kosten und mehr Komplexität zu verursachen. Um festzustellen, ob diese Anforderung erfüllt ist, müssen in Unternehmen folgende Fragen gestellt werden:

1. Kann die Lösung Anwendungen von der Cloud bis zum Endbenutzer konsistent priorisieren? Ein isolierter Ansatz zur Bestimmung der Quality of Service für Anwendungen liefert nur unzureichende Ergebnisse. Eine konsistente Priorisierung der Anwendungen von der Cloud über private oder öffentliche Netzwerke bis zum Endbenutzergerät ist für eine konsistent hohe Benutzerfreundlichkeit unverzichtbar.

2. Kann die Lösung den Aufbau neuer Außenstellen oder Segmente mit eingeschränktem lokalem Support unterstützen? Der Aufbau eines Netzwerks an einem Remote-Standort mithilfe eines Technikereinsatzes ist ein teures und zeitaufwändiges Vorhaben. Digitale Unternehmen arbeiten so schnell, dass beim Aufbau neuer Außenstellen, Netzwerksegmente oder Funktionen nicht gewartet werden können, bis die neuen Komponenten vor Ort von einem Techniker angeschlossen und konfiguriert wurden. Plug-and-Play-Funktionen und sofortige Bereitstellung sind entscheidend, um Zeit und Kosten einzusparen.

3. Können neue Funktionen und Standards ohne großflächiges Upgrade hinzugefügt werden? Wenn neue Funktionen ohne den fortlaufenden Austausch alter Infrastrukturkomponenten durch neue Geräte hinzugefügt werden können, lassen sich Betriebsunterbrechungen minimieren und erhebliche Kosteneinsparungen erzielen. Außerdem müssen Netzwerkmanager in der Lage sein, Software-Updates ohne Unterbrechungen für Benutzer anzuwenden, damit die Produktivität nicht beeinträchtigt wird. Investitionen in Lösungen, mit denen Funktionen schnell und einfach erweitert werden können, sind zur Erfüllung neuer Geschäftsanforderungen unverzichtbar.

4. Können Lizenzen problemlos übertragen werden? Unternehmen müssen in der Lage sein, Hardware zu aktualisieren, ohne dass zusätzliche Kosten durch den Erwerb neuer Softwarelizenzen entstehen. Eine Trennung der Softwarelizenz von der Hardware ist äußerst wichtig, da Unternehmen ihre Netzwerkinfrastruktur aufgrund schneller steigender Anforderungen häufiger aktualisieren müssen.

Die Bedrohungserkennung stellt weiterhin eine große Herausforderung für Unternehmen dar.

Können mithilfe des Netzwerks die Sicherheit erhöht und Risiken minimiert werden?

Das Netzwerk kann als wertvoller Ausgangspunkt dienen, um nicht nur den Benutzerzugriff zu erteilen, sondern auch die Benutzeraktivitäten anhand von umfassendem Kontext zu validieren. Die Bedrohungserkennung stellt weiterhin eine große Herausforderung für Unternehmen dar. Laut Security Survey 2016 von ZK Research beträgt die durchschnittliche Zeit zur Lokalisierung einer Sicherheitsverletzung mehr als 100 Tage. Unternehmen benötigen Wege, Bedrohungen schon nach wenigen Stunden statt erst nach mehreren Tagen zu erkennen. Dazu sollten folgende Fragen gestellt werden:

1. **Kann die Lösung mithilfe eines softwarebasierten Ansatzes den Datenverkehr logisch segmentieren und bei Erkennung neuer Risiken automatisch angepasst und skaliert werden?** Netzwerksegmentierung wird zunehmend von Kunden eingesetzt, die Benutzer- und Anwendungsdatenverkehr in sicheren Zonen isolieren möchten. Mitarbeitern, Gästen, Dienstleistern und IoT-Geräten den Zugriff auf benötigte Ressourcen zu erteilen, ist bei Verwendung von Zugriffskontrolllisten und RADIUS in kleineren Bereitstellungen relativ unkompliziert. Bei steigenden Benutzer- und Gerätezahlen ist die Verwaltung dieser Listen jedoch wenig praktikabel. Neue digitale Unternehmen segmentieren den Datenverkehr logisch anhand von Benutzertyp und -rolle. So können sie ihre Zugriffsrichtlinie schnell anpassen und je nach Risiko automatisch Anpassungen vornehmen.

2. **Verfügt die Lösung über in die Netzwerkinfrastruktur integrierte Sicherheitsfunktionen zur Erkennung interner und externer Bedrohungen hinsichtlich Zugriff, Core, WAN und Außenstelle?** Laut Network Purchase Intention Study 2016 von ZK Research waren 78 Prozent der Befragten nicht überzeugt, dass in der IT-Abteilung sämtliche mit dem Netzwerk verbundenen IoT-Geräte bekannt sind. Bei der Automatisierung der Erkennung von IoT-Endpunkten ist das Netzwerk eine wertvolle Ressource. Mithilfe von Traffic-Analysen können außerdem Benutzer- und IoT-Aktivitäten überwacht werden. Abweichungen vom normalen Verhalten können auf schädliche Aktivitäten oder eine mögliche Sicherheitsverletzung hinweisen.

3. **Kann die Lösung durch die Analyse von Traffic-Flüssen die Auswirkungen von Bedrohungen beseitigen?** Jedes Unternehmen wird früher oder später mit Bedrohungen konfrontiert. Die Auswirkungen dieser Bedrohungen können schon in kürzester Zeit den gesamten Geschäftsbetrieb lahmlegen. Daher müssen Unternehmen die herkömmliche Bedrohungserkennung und -analyse hinter sich lassen. Mithilfe von Daten aus dem Netzwerk können die Ursache und der Ort eines Angriffs identifiziert und dessen Auswirkungen umgehend beseitigt werden. Im Fall einer Sicherheitsverletzung kann der Datenverkehr am Netzwerkübergang zur weiteren Prüfung schnell gespiegelt werden.

4. **Kann die Lösung Informationen zu neuen Bedrohungen konsistent aktualisieren, bevor diese im Netzwerk auftreten?** Bei einem reaktiven Ansatz zur Risikoreduzierung erfolgt eine Benachrichtigung erst, wenn bereits schädliche Aktivitäten im Netzwerk stattfinden. Unternehmen können neuen Bedrohungen einen Schritt voraus bleiben, wenn sie kontinuierlich externe Bedrohungsinformationen erfassen und damit das System automatisch aktualisieren, um Sicherheitsverletzungen vorzubeugen. Netzwerk- und Sicherheitsexperten müssen ihre reaktive Sicherheitsstrategie in eine proaktive umwandeln, um das Risiko einer Sicherheitsverletzung zu verringern. Sollte dennoch eine Sicherheitsverletzung stattfinden, können Tools zur Datenerfassung und -analytik die Malware schnell auffinden und automatisch Änderungen am Netzwerk vornehmen, um die Auswirkungen zu minimieren.

Nur etwa 20 Prozent der Gesamtkosten für den Betrieb eines Netzwerks entfallen auf die Hardware, während die Betriebskosten mindestens 50 Prozent ausmachen.

Wie sollte das Netzwerk verwaltet werden?

Diese Frage wird in vielen Unternehmen häufig vernachlässigt, obwohl sie eine der wichtigsten Fragen überhaupt ist. Die Kosten der Netzwerkgeräte stehen in der Regel besonders im Fokus, obwohl nur etwa 20 Prozent der Gesamtkosten für den Betrieb eines Netzwerks auf die Hardware entfallen, während die Betriebskosten mindestens 50 Prozent ausmachen.

Bisher wurden Netzwerke geräteweise über eine Kommandozeile verwaltet. Die Umsetzung von Änderungen im Netzwerk gestaltete sich langwierig und mühsam. Umfragen von ZK Research zufolge beträgt die durchschnittliche Zeit zur Implementierung einer netzwerkweiten Änderung ganze vier Monate – für digitale Unternehmen viel zu lang. Außerdem sind menschliche Fehler für 35 Prozent der Netzwerkausfälle verantwortlich und damit die größte Ursache von Ausfällen. Auch das Netzwerkmanagement muss sich im digitalen Zeitalter verändern. Netzwerkmanager sollten eine Lösung mit folgenden Funktionen in Betracht ziehen:

Einheitliches kabelgebundenes und Wireless-Management

Netzwerkweite anstatt geräteorientierte Bereitstellung

Funktionsreiche grafische Benutzeroberfläche, damit fachfremde Techniker grundlegende Konfigurationsänderungen vornehmen können

Möglichkeit zum Rückgängigmachen von Konfigurationsänderungen bei Bedarf

Sowohl standort- als auch Cloud-basierte Managementfunktionen, um Kunden unterschiedliche Managementmodelle anbieten zu können

IV: ZUSAMMENFASSUNG UND EMPFEHLUNGEN

Digitale Trends haben den Wert des Netzwerks erhöht. Daher sollte es nicht mehr als geringwertige Ressource oder „Massenware" betrachtet werden. Der Netzwerkübergang ist die Schnittstelle, über die Benutzer auf Anwendungen und Inhalte zugreifen. Das macht ihn zu einer strategischen Ressource mit Potenzial für einen Wettbewerbsvorteil. IT-Abteilungen und Führungskräfte müssen sämtliche Aktivitäten am Netzwerkübergang berücksichtigen und auf dieser Grundlage handelsübliche Infrastruktur gegen Premium-Netzwerke von Anbietern wie Cisco abwägen.

Kostengünstige Netzwerkgeräte mögen zwar auf den ersten Blick attraktiv erscheinen, verursachen jedoch langfristig größere Sicherheitsrisiken, beschränken die Möglichkeit zur Überwachung und Optimierung der Anwendungsleistung und sind kaum in der Lage, Prozesse zu automatisieren. All dies sind jedoch wichtige Voraussetzungen für Erfolg im digitalen Zeitalter. Aus diesem Grund müssen Unternehmen am Netzwerkübergang die richtige Wahl treffen, um eine solide Grundlage für die Digitalisierung zu schaffen. Daher gibt ZK Research folgende Empfehlungen:

Berücksichtigen Sie beim Kauf von Netzwerkgeräten die Gesamtbetriebskosten, nicht die Anschaffungskosten. Daten von ZK Research zufolge entfallen nur etwa 20 Prozent der Gesamtkosten für den Betrieb eines Netzwerks auf die Hardware, während die Betriebskosten 50 Prozent ausmachen. Geringfügige Einsparungen bei der Hardware können also erhebliche Probleme beim Betrieb nach sich ziehen und dadurch die Gesamtbetriebskosten ansteigen lassen.

Analysieren Sie die Auswirkungen des Netzwerks auf die Betriebsabläufe. Um die Rolle des Netzwerkübergangs angemessen beurteilen zu können, ist ein klares Verständnis der Kosten durch geplante und ungeplante Ausfallzeiten im Unternehmen erforderlich. Sämtliche Ausfallzeiten oder Leistungsprobleme beeinträchtigen die Produktivität der Mitarbeiter und führen zu Kundenabwanderung. Eine Sicherheitsverletzung kann die Marke erheblich beschädigen und sogar zu Rechtsstreitigkeiten führen.

Treffen Sie eine zukunftssichere Entscheidung für den Netzwerkübergang. Machen Sie sich bewusst, welche Anwendungen und Kommunikationsservices in Ihrem Unternehmen heute verwendet werden und was in Zukunft genutzt werden soll (Video, IP-Sprachdienste, Messaging, Mobilität, IoT usw.). Wählen Sie dann den Anbieter, der Ihnen die beste Gesamtlösung liefern kann. Diese dient als Grundlage für digitale Services und Anwendungen.

KONTAKT

zeus@zkresearch.com

Mobil: +1 301 775-7447
Büro: +1 978 252-5314