

OPTIMIEREN UND SICHERN SIE IHR HYBRIDES NETZWERK

Vier Schritte, um Disruption in der Neuen Zukunft zu überwinden und ein agiles, sicheres sowie skalierbares Netzwerk zu schaffen.



Einleitung

Die Welt verändert sich gerade. Umbrüche durchziehen die globale Wirtschaft. Wie bei jeder wirtschaftlichen Disruption bietet dies agilen, innovativen Organisationen die Möglichkeit, solche Umbrüche in einen Wettbewerbsvorteil zu verwandeln. Dieses Papier beleuchtet die Netzwerk- und Sicherheitsprioritäten, mit denen sich Unternehmen heute, beim Übergangsprozess der "Rückkehr zur Arbeit im Büro " und in der Neuen Zukunft befassen müssen.





Übersicht

+ HEUTE

Es gilt, die Kontinuität des Geschäftsbetriebs und ein höchstmögliches Maß an Kundenerlebnis und interner Benutzererfahrung sowie gleichzeitig die unternehmensweite Sicherheit zu gewährleisten – und dies muss angesichts eingefrorener Budgets und Ressourcen umgesetzt werden.

+ DIE RÜCKKEHR IN DEN BÜROALLTAG

Der Wechsel zum Homeoffice geschah für die meisten Organisationen innerhalb weniger Tage. Aber die Rückkehr an den Arbeitsplatz oder genauer gesagt, die Rückkehr ins Büro, wird ein Prozess sein, der sich über mehrere Monate hinzieht und für viele Arbeitnehmer ein neues, bewegliches Arbeitsumfeld voraussetzt.

+ DIE NEUE ZUKUNFT

Angesichts globaler Umbrüche, Unsicherheiten und Herausforderungen haben Unternehmen die Möglichkeit, ihre Geschäftsmodelle neu zu überdenken und digitale Initiativen zu beschleunigen oder zu lancieren, die es ihnen ermöglichen, aus dieser Situation stärker hervorzugehen. Sie müssen dafür entsprechende Konzepte entwickeln, die eine Reihe möglicher zukünftiger Zustände berücksichtigen und eine agile Netzwerk- und Sicherheitsinfrastruktur aufbauen, die diese Vorhaben unterstützt.

Wir möchten Ihnen unsere Vorschläge dazu aufzeigen, wie Organisationen am besten durch diese beispiellosen Zeiten navigieren können. Diese basieren auf den Erfahrungen, die wir mit unserem Kundenstamm aus führenden Unternehmen und Organisationen in allen Branchen machen.

Heute

Nun, da sich die ersten Veränderungen in Bezug auf die Arbeit im Homeoffice eingependelt haben und die weitere Richtung in den Fokus gerückt ist, sieht sich die IT mit einer Reihe neuer Herausforderungen konfrontiert, die sich aus vier unternehmerischen Notwendigkeiten ergeben.

Liefere Sie das bestmögliche Kundenerlebnis

Die Gewährleistung der bestmöglichen Customer Experience ist ein wesentliches Ziel, unabhängig davon, ob eine Organisation im Gesundheits- oder Bankwesen, beim Online-Handel, bei der Lieferung von Lebensmitteln oder in einem der unzähligen anderen Dienstleistungsbereiche tätig ist, auf die Kunden heutzutage von zu Hause angewiesen sind.

Die Bereitstellung dieses Niveaus der Customer Experience bedeutet eine Kombination aus Beschleunigung von Initiativen zur digitalen Transformation, die Umstellung bestehender Anwendungen auf skalierbare cloudbasierte Architekturen oder die Einführung neuer SaaS-basierter Online-Applikationen. Die meisten Unternehmen hatten diese Initiativen bereits vor der aktuellen Krise auf den Weg gebracht. Viele suchen jetzt jedoch nach Möglichkeiten, diese Initiativen zu beschleunigen oder neue Initiativen zu starten, mit denen sie ihr Geschäft auf einer neuen digitalen Plattform neu konzipieren können.

Mehr mit weniger erreichen

Eine der Herausforderungen bei der Bereitstellung des bestmöglichen Kundenerlebnisses durch die Beschleunigung von Initiativen zur digitalen Transformation besteht darin, dass die meisten Unternehmen mit eingefrorenen oder reduzierten Budgets und begrenzten Ressourcen arbeiten müssen, unabhängig davon, ob sie unmittelbar vom wirtschaftlichen Abschwung betroffen oder von der allgemeinen Abschwächung der Konjunktur eingeholt wurden.

Als Reaktion darauf arbeiten viele CIOs mit den Finanzteams ihrer Unternehmen zusammen, um die CapEx- und OpEx-Kosten zu durchleuchten und diese Investitionen neu zu priorisieren. Damit soll sichergestellt werden, dass kritische Sicherheits- und Initiativen zur Digitalisierung realisiert werden können.

Parallel zur Neupriorisierung der Projektausgaben müssen IT-Organisationen auch ihre bestehende Infrastruktur, Tools und Anwendungen optimieren, um OpEx-Kosten und Ressourcen freizusetzen, die besser für kundenorientierte oder digitale Transformationsinitiativen mit höherem Wirkungsgrad eingesetzt werden könnten.

Unterstützen Sie den flexiblen Arbeitsplatz

Für viele Organisationen in allen Industrie- und öffentlichen Sektoren wird das Homeoffice-Modell nicht nur Teil ihrer langfristigen Planung, sondern zur Grundlage ihres „flexiblen“ Arbeitsplatzes sein, der Homeoffice- und Büroarbeitsplätze nahtlos zusammenführt.

Das bedeutet, dass Funktionen, die zur Unterstützung von WFH (Work From Home) ohne detaillierte Planung eingeführt wurden, wie z.B. die zunehmende Inanspruchnahme von SaaS-basierten Videokonferenz- und Kollaborationsanwendungen, nun in bürobasierte Systeme integriert werden müssen, damit die Mitarbeiter ohne Produktivitätsverlust zwischen diesen Umgebungen wechseln können.

Sichern Sie das neue Netzwerk

Gefährder nutzten die vorherrschende Atmosphäre aus Paranoia und Unsicherheit unmittelbar nach der Pandemie schnell aus und entfesselten eine Welle von Phishing-, Malware- und Ransomware-Angriffen. Diese Angriffe traten in dieser Zeit häufig auf, da viele Organisationen mit der Herausforderung des Homeoffice-Modells zu kämpfen hatten. Dazu zählten VPN-Fähigkeiten und BYOD-(Bring Your Own Device)-Laptops, Telefone und Heimnetzwerke mit unzureichender Endpunkt-Sicherheit.

Da diese Sicherheitsfragen eine so hohe Priorität hatten, reagierten die meisten Organisationen entschlossen und erhöhten die Sicherheitsausgaben und -ressourcen, um diese Probleme zu lösen. Mit dem Übergang von Organisationen zu einem flexiblen Arbeitsplatzmodell wird es jedoch neue Herausforderungen geben, die erfordern, dass die InfoSec-Teams volle Sichtbarkeit und Kontrolle über ein breiteres Spektrum von Geräten, Benutzern, Applikationen und Daten haben müssen als jemals zuvor.

Die Rückkehr zum Arbeitsplatz im Unternehmen

Genauso wie der Zeitpunkt des Übergangs zum Homeoffice von Land zu Land und von Region zu Region unterschiedlich war, wird auch die Rückkehr an den Arbeitsplatz oder genauer gesagt die Rückkehr ins Büro variieren.

Die meisten Organisationen planen jetzt den Prozess der Rückkehr in die Büros und haben funktionsübergreifende Teams gebildet, wobei die IT ein wesentlicher Bestandteil dieser Teams und dieses Prozesses ist. Doch worauf sollten sich IT-, NetOps- und InfoSec-Teams konzentrieren, während diese Pläne entwickelt werden? Wenn wir uns Gigamon Kunden ansehen, sehen wir, dass sie sich auf Projekte konzentrieren, die in drei große Bereiche aufgeteilt sind.

Planen Sie die Rückkehr zum Arbeitsplatz im Unternehmen

Viele Organisationen planen eine Zukunft, in der eine beträchtliche Anzahl ihrer Mitarbeiter weiterhin von zu Hause aus arbeiten wird, entweder auf permanenter Basis oder für einen längeren Zeitraum als Teil eines gemischten Onsite-/Offsite-Modells, das nun als „flexibler Arbeitsplatz“ beschrieben wird.

Eine im März¹ durchgeführte Umfrage der 451 Group deutete darauf hin, dass 38 Prozent der Befragten erwarteten, dass dies die neue Norm für ihre Organisation werden wird. Eine Umfrage, die während eines jüngsten Gigamon Webinars² zum Gesundheitswesen durchgeführt wurde, deutete jedoch darauf hin, dass dies bis zu 75 Prozent so

sehen könnten. Darüber hinaus berichten viele Organisationen, dass Mitarbeiter, die zu Hause arbeiten, entgegen den Erwartungen vieler Menschen, tatsächlich produktiver sind als Mitarbeiter im Büro.

Diese Produktivität wird weitgehend durch die effektive Nutzung einfach zu bedienender, sicherer und skalierbarer SaaS-basierter Anwendungen wie Videokonferenzen und Kollaborationsapplikationen erreicht, die Internet- und Mobilfunknetze mit hoher Bandbreite nutzen und ältere desktopbasierte Anwendungen rasant ersetzen. IT-Organisationen müssen sicherstellen, dass sie sowohl in Homeoffice- als auch in Büroumgebungen eine nahtlose Nutzungsmöglichkeit für ihre Mitarbeiter sicherstellen können.

Nutzen Sie die Cloud, um die digitale Transformation zu beschleunigen

Initiativen zur digitalen Transformation sind von Natur aus cloudbasiert, da die Cloud die schnellste Bereitstellung neuer Anwendungen und digitaler Dienste ermöglicht. Um jedoch die reichhaltigste Funktionalität und die beste Customer Experience zu bieten, erstrecken sich diese cloudbasierten Anwendungen oft über physische, virtuelle, Cloud- und Multi-Cloud-Netzwerke.

Diese Initiativen können auf SaaS-basierten Anwendungen aufbauen, oder sie können auf benutzerdefinierten Anwendungen beruhen, die von internen IT-Organisationen entwickelt und für eine schnelle Skalierbarkeit auf cloud- und containerbasierten Plattformen bereitgestellt werden. Um dies zu erreichen, müssen alle Daten – sowohl verschlüsselte als auch unverschlüsselte – sichtbar sein, während sie die verteilten Ebenen der Anwendung durchlaufen, einschließlich der Kommunikation zwischen den Containern.



Eine Umfrage, die während eines jüngsten Gigamon Webinars zum Gesundheitswesen erfolgte, ergab, dass **75 Prozent der Umfrageteilnehmer erwarten, dass das Homeoffice die neue Norm sein wird.**



Wenn Probleme mit der Performance von Anwendungen auftreten, ist es oft notwendig, über die Fragen der Netzwerkbandbreite hinauszublicken und beispielsweise herauszufinden, warum sich die Frameraten verlangsamen oder die Qualität von HD auf SD sank. In diesen Fällen kann die Funktion zur Verwendung der Metadaten innerhalb der Anwendung entscheidend sein, um festzustellen, wo potenzielle Engpässe oder andere Probleme bestehen, die eine schlechte Performance und eine schlechte User Experience verursachen.



Die Verfügbarkeit der Metadaten innerhalb der Anwendung kann entscheidend sein.

Bewerten Sie die Sicherheit neu

Jetzt ist der ideale Zeitpunkt für die InfoSec-Teams, die aus der Reaktion auf diese Krise gezogenen Lehren auszuwerten und diese auf eine Überprüfung ihrer bestehenden Sicherheitsmodelle, Verfahren und Tools anzuwenden. Diese Modelle standen wahrscheinlich schon vor der COVID-19-Krise aufgrund der folgenden Punkte unter Stress:

- + Unterbesetzte InfoSec- und SecOps-Teams³
- + Rasantes Wachstum im verschlüsselten Nord-Süd- und Ost-West-Datenverkehr
- + Massive Zunahme des Datenverkehrs und der Angriffsfläche, oft als Folge der Einführung von OT und IoT

Zu diesen Problemen kommt nun noch der zusätzliche Stress hinzu, den die Krise auf das Sicherheitspersonal, -Tools und das Budget ausgeübt hat.

Während das genaue Sicherheitsmodell von Organisation zu Organisation variiert wird, sind die wichtigsten Bausteine für ein erfolgreiches, agiles Modell die Gewährleistung einer Ende-zu-Ende-Sichtbarkeit des gesamten Netzwerkverkehrs, KI- und ML-basierte Analysetools, die Anomalien und Bedrohungen erkennen und priorisieren, sowie Automatisierungswerkzeuge, die alltägliche Aufgaben bewältigen, so dass sich die Sicherheitsteams auf die Fragen mit höchster Priorität konzentrieren können.

Für einige Organisationen kann diese Sicherheitsüberprüfung eine Evaluierung der Einführung eines Zero-Trust-Modells beinhalten. In einer Welt, in der das flexible Arbeitsplatzmodell die neue Norm ist, ist die Entwicklung hin zu einer Zero-Trust-Architektur nicht nur sinnvoll, sondern auch nahe an einem Gebot. Auf der einfachsten Ebene müssen alle Benutzer, Geräte, Anwendungen und Ressourcen als feindlich behandelt werden, da das Netzwerk ständig von einer Vielzahl von externen und internen Bedrohungen angegriffen wird. Diese Benutzer und Geräte müssen rigoros authentifiziert werden, und Daten und andere Netzwerkressourcen müssen auf einer viel granulareren Ebene geschützt werden, als es perimeterbasierte Sicherheitsmodelle zulassen.

Optimieren Sie Ihre Bandbreite

Die Kombination aus der Unterstützung der Rückkehr zum Arbeitsplatz im Büro bei gleichzeitiger Förderung der digitalen Transformation und Gewährleistung der unternehmensweiten Sicherheit bedeutet, dass alle Unternehmen die Netzwerkbandbreite und die Sichtbarkeit des Netzwerkverkehrs maximieren müssen. Die Erhöhung der Netzwerkbandbreite kann entweder durch Aufrüstung oder Ersatz der vorhandenen Netzwerkinfrastruktur oder durch Optimierung der vorhandenen Bandbreite erreicht werden. Häufig ist die Optimierung der vorhandenen Bandbreite eine kurzfristige Maßnahme, die Unternehmen ergreifen müssen, während sie mittelfristig ein Netzwerk-Upgrade planen.

Für die Optimierung der Netzwerkbandbreite ist das Verständnis dessen, welche Anwendungen und welcher Datenverkehr auf dem gegenwärtigen Netzwerk laufen und wie dieses in Zukunft wahrscheinlich wachsen wird, von grundlegender Bedeutung. Um dies zu erreichen, ist Sichtbarkeit über alle Benutzer und Anwendungen im Netzwerk erforderlich. Dies betrifft das Rechenzentrum genauso wie mobile oder Homeoffice-Arbeitsplätze oder Daten in der Cloud. Sobald diese Sichtbarkeit erlangt wurde, ist es möglich, den Netzwerkverkehr zu verstehen, den sie erzeugen und verbrauchen.

Dieses Verständnis ermöglicht kurzfristig eine Optimierung des Datenverkehrs durch Techniken wie Deduplizierung, Filterung, Slicing und Verwendung von Metadaten. Derselbe Prozess bietet eine solide Grundlage für die Planung der Kapazität, die benötigt wird, um den zukünftigen Netzwerkbedarf der Organisation zu decken. Die Projektion der Netzwerkkapazität für die Netzwerke von morgen ist keine leichte Aufgabe, aber eine detaillierte Sichtbarkeit des heutigen hybriden Netzwerkverkehrs ist ein wesentlicher erster Schritt.



Die Entwicklung hin zu einer Zero-Trust-Architektur macht nicht nur Sinn, sondern ist nahe an einem Gebot.

Die Neue Zukunft

Jede wirtschaftliche Krise bietet agilen, innovativen Organisationen die Möglichkeit, genau diese Krise in einen Wettbewerbsvorteil zu verwandeln. Heute bedeutet dies, dass digitale Technologien eingesetzt werden müssen, um die Art und Weise, wie Unternehmen mit ihren Kunden interagieren und Geschäfte abwickeln, schneller, bequemer und kostengünstiger als ihre Wettbewerber zu gestalten.

Die meisten Organisationen hatten bereits vor der gegenwärtigen Krise Initiativen für die digitale Transformation auf den Weg gebracht. Diejenigen Organisationen, die aus dieser Situation am stärksten hervorgehen, werden jedoch jene sein, die diese Initiativen wiederholen oder sogar neu beginnen, indem sie ihr Geschäft auf einer neuen digitalen Plattform aufbauen. Eine der Herausforderungen dabei ist heute, dass viele Organisationen mit eingefrorenen Budgets und begrenzten Ressourcen arbeiten müssen.



SICHTBARKEIT

Wie die jüngsten Ereignisse gezeigt haben, bedeutet Agilität nicht einfach nur, mit dem Druck von Wachstum und Innovation umzugehen; es bedeutet auch, unvorhergesehene und beispiellose Veränderungen zu meistern. In dieser Situation ist es von entscheidender Bedeutung, dass die Netzwerke und Sicherheitskapazitäten der Organisationen kontinuierliche Veränderungen der Arbeitspraktiken und den Einsatz neuer Tools unterstützen können.



WACHSTUM

Organisationen, die diese Merkmale von Agilität, Sichtbarkeit und Innovation aufweisen und operationalisieren, werden aus der gegenwärtigen Situation stärker hervorgehen und für ein schnelles organisches und akquisitionsbasiertes Wachstum bereit sein. Um dies zu erreichen, werden sie agile, skalierbare Netzwerke und Tools wie die Gigamon Visibility and Analytics Fabric™ benötigen, die vollständige Sichtbarkeit in den Anwendungen, Benutzern und Daten bieten, die über physische, virtuelle, Cloud- und Multi-Cloud-Netzwerke verteilt sind.



AGILITÄT

Was man nicht sehen kann, kann man nicht managen. Somit ist der Einblick in den gesamten Netzwerkverkehr für viele Organisationen zu einer Überlebensfrage geworden. Der physischen, virtuellen und cloudbasierten Sichtbarkeit, die Gigamon sowohl in verschlüsselte als auch in unverschlüsselte Daten bietet, wird bereits von vielen der anspruchsvollsten Organisationen der Welt vertraut. Darunter sind führende globale Banken, das Gesundheitswesen, Service Provider, SaaS-Unternehmen und Regierungsbehörden.



CLOUD

Die meisten IT-Organisationen in einer Welt der Neuen Zukunft sind mit Budget-Unsicherheiten konfrontiert. Agil und schlank zu sein, ist mehr denn je nicht nur für Altsysteme, sondern auch für neue Systeme in der Cloud entscheidend. Gigamon ermöglicht es der IT, aus bestehenden Investitionen mehr herauszuholen und so im laufenden Geschäftsjahr ein zusätzliches, frei verfügbares Budget zu generieren. Gigamon erhöht beispielsweise durch das Entfernen von doppeltem Datenverkehr, dem Herausfiltern risikoarmen Anwendungsverkehrs und indem Teams erlaubt wird, zurückgestellte Tools neu bereitzustellen, sofort die Kapazitäten von Monitoring- und Security-Tools um bis zu 70 Prozent.



Einige Gedanken zum Schluss

Die COVID-19-Krise hat eine Kettenreaktion an Ereignissen ausgelöst, die unsere Gesellschaft und Wirtschaft tiefgreifend beeinflussen werden. Organisationen und ihre IT-Teams haben erfolgreich auf den ersten von der Krise ausgelösten Schock reagiert. Die härtesten Herausforderungen – und die größten Chancen – liegen noch vor uns. Um diese Herausforderungen zu überleben und sie als Chancen zu nutzen, brauchen Organisationen Widerstandsfähigkeit, Beweglichkeit und Sichtbarkeit in jeden Aspekt ihrer Arbeit. Gigamon ist einzigartig aufgestellt, sodass wir unseren Kunden bei der Bewältigung dieser Herausforderungen so helfen können, dass sie davon sogar profitieren. Dies können wir tun, indem wir ihre digitale Reise beschleunigen und ihnen gleichzeitig ermöglichen, mit weniger mehr zu erreichen.

¹ Scott Crawford, Dan Kennedy, Fernando Montenegro, Eric Hanselman, Garrett Bekker and Aaron Sherrill. "COVID-19 and Beyond: Will the Work-From-Home Explosion Revolutionize Enterprise Security Architecture?" April 2, 2020. 451 Research. <https://go.451research.com/2020-mi-covid-19-will-work-form-home-revolutionize-enterprise-security-architecture.html>.

² Die Umfrage wurde während eines HIMSS Gigamon Webinars am 22. April 2020 erhoben.

³ "2020 Cyberthreat Defense Report." März 2020. CyberEdge Group. <https://cyber-edge.com/wp-content/uploads/2020/03/CyberEdge-2020-CDR-Report-v1.0.pdf>.

Über Gigamon

Gigamon bietet Netzwerksichtbarkeit und -Analyse allen Datenverkehrs über Ihr physisches, virtuelles und cloudbasiertes Netzwerk, um wichtige sicherheitsrelevante, funktionelle und den Geschäftsbetrieb erhaltene Probleme zu lösen. Die Gigamon Visibility and Analytics Fabric™ bietet eine optimierte Netzwerk- und Security-Performance, erleichtertes Management und beschleunigte Fehlerbehandlung. Dabei wird der ROI Ihrer Tools erhöht. Unsere umfassenden Lösungen beschleunigen die Fähigkeit Ihres Unternehmens, Sicherheitsbedrohungen zu erkennen und darauf zu reagieren, einschließlich derer, die im verschlüsselten Datenverkehr versteckt sind. Mehr als 82 Prozent der Fortune 100 und insgesamt 4.000 Unternehmen auf der ganzen Welt vertrauen auf Gigamon. Gigamon sorgt dafür, dass Ihr Unternehmen schnell arbeiten kann und in der Neuen Zukunft sicher bleibt.

©2017-2020 Gigamon. Alle Rechte vorbehalten. Gigamon und das Gigamon Logo sind Warenzeichen von Gigamon in den Vereinigten Staaten und/oder anderen Ländern. Gigamon Markenzeichen können unter www.gigamon.com/legal-trademarks gefunden werden. Alle anderen Marken sind die Marken ihrer jeweiligen Eigentümer. Gigamon behält sich das Recht vor, diese Publikation ohne vorherige Ankündigung zu ändern, zu modifizieren, zu übertragen oder anderweitig zu überarbeiten.

Gigamon®

Globales Hauptquartier
3300 Olcott Street, Santa Clara CA, 95054 USA
+1 (408) 831-4000 | www.gigamon.com