Grundlagen einer skalierbaren und langfristigen Strategie für sicheren Remote-Zugriff und Telearbeit in der Post-COVID-19-Ära

Einführung

Fast über Nacht hat sich im ersten Halbjahr 2020 die Arbeitsweise der meisten Unternehmen verändert. Aufgrund der COVID-19-Pandemie ist es heute für Unternehmen auf der ganzen Welt zur „neuen Normalität" geworden, dass die meisten Mitarbeiter von zu Hause aus arbeiten. Dies führt zu einer stärkeren Beanspruchung des Netzwerks und anderen Problemstellungen für die IT- und Sicherheitsteams, da die Mitarbeiter auch weiterhin einen sicheren Zugriff auf Anwendungen und Daten benötigen.

In Sachen Sicherheit besteht die größte Herausforderung für Unternehmen darin, ihre Mitarbeiter von zu Hause aus arbeiten zu lassen – und den Rattenschwanz an Problemen zu bewältigen, den dies nach sich zieht. Diese reichen von fehlerhaften Konfigurationen bis hin zu einem Mangel an Cybersicherheitsspezialisten und einer größeren Gefährdung durch Phishing-Angriffe.

Viele Unternehmen lassen ihre Mitarbeiter bereits von zu Hause aus arbeiten – und zwar über VPNs und mit vom Unternehmen kontrollierten Endpoints. Dies war jedoch nie auf die heute erforderliche Größenordnung ausgelegt. Daher greifen Mitarbeiter ohne die richtige Sicherheitsinfrastruktur auf wichtige Ressourcen zu.

AUF EINEN BLICK

DAS WICHTIGSTE

Ein Zero-Trust-Netzwerkzugang (ZTNA) bietet mehrere Vorteile für groß angelegte Telearbeitsstrategien:

- kein Bedarf an teuren, komplizierten und nicht skalierbaren VPN-Lösungen mehr
- gleiche Benutzererfahrung wie im Büro
- geringeres Risiko durch Dritte, indem Benutzer und Anwendungen mit den entsprechenden Berechtigungen Zugriff erhalten

Unternehmen müssen ihren Mitarbeitern überall dieselbe Arbeitsumgebung, die gleiche Performance und die gleiche Benutzererfahrung bieten wie im Büro – und all das auf sichere Weise.

In den meisten Fällen wird das Problem durch den Ausbau bestehender Lösungen nur kurzfristig aufgeschoben, damit einstweilen alles „funktioniert". Eine skalierbare, langfristige Lösung ist das allerdings nicht. Um den Sicherheitsanforderungen gerecht zu werden, müssen es die Unternehmen ihren Mitarbeitern ermöglichen, effizient und sicher und ohne Abstriche bei der Benutzerfreundlichkeit von zu Hause aus zu arbeiten. Im Umgang mit COVID-19 verfolgen Sicherheitsteams zwei unterschiedliche Ansätze: Entweder den Ausbau bestehender Lösungen (VPNs mit kontrollierten Endpoints) oder aber die Implementierung eines „Break-Glass"-Ansatzes, um Mitarbeiter bei der Arbeit mit sicherem Netzwerkzugriff zu unterstützen, wenn sie z. B. Büro-PCs mit nach Hause nehmen oder gebeten werden, ihre eigenen PCs zu verwenden (BYOPC) oder Fernwartungstools zum Einsatz kommen usw.

Laut der weltweiten Befragung *COVID-19 Impact on IT Spending Survey* (April 2020) von IDC sind 47 Prozent aller Unternehmen der Ansicht, dass die Nachfrage nach sicherem Fernzugriff im Zusammenhang mit COVID-19 steigt und dass neue Technologien und Änderungen am Arbeitsmodell ihres Unternehmens erforderlich wären. Was die Ausgaben in Europa anbetrifft, so hat die in Europa durchgeführte IDC-Befragung *Impact of COVID-19 on the European ICT Market and Ecosystem* (März 2020) ergeben, dass Collaboration-Technologien (+57 Prozent) und Sicherheit (+16 Prozent) die beiden wichtigsten IT-Bereiche waren, in denen Unternehmen für 2020 ein Wachstum erwarteten.

Unternehmen entwickeln nun ihre neuen Business-Continuity-Pläne und schreiten zu einer Neubewertung ihrer Optionen. Ihre bestehenden Lösungen für die Remote-Arbeit, die Optionen für Telearbeit in großem Umfang wie während der Lockdowns, Optionen für Mitarbeiter von Dritten (Auftragnehmern, Kunden usw.) und die Organisation der Fernwartung müssen einzeln und jeweils für sich genommen überdacht werden. Die Unternehmen müssen dies als einen einzigen großen Problembereich betrachten – mit einer „massentauglichen" Lösung für die Fernarbeit und einem „allgemeineren" Business-Continuity-Plan. In den meisten Fällen werden sie eine (oder mehrere) Lösungen für die Zukunft benötigen, und diese wird sich wahrscheinlich radikal von den Lösungen der Vergangenheit unterscheiden.

Vorteile

Ein Zero-Trust-Netzwerkzugriff (ZTNA) ist nicht nur eine Sicherheitslösung für den Netzwerkzugriff, sondern bringt unmittelbare Vorteile, die das Unternehmen auch geschäftlich weiterbringen können.

Eine benutzerfreundliche Lösung steigert die Produktivität des Unternehmens, da sich Remote-Mitarbeiter in einer Umgebung befinden, die mit ihrer vom Büro gewohnten Umgebung identisch ist, ohne Verzögerungen oder Zugriffsprobleme aufgrund langsamer Netzwerke. Eine skalierbare Lösung, die einerseits die vergleichsweise kleine Anzahl herkömmlicher Remote-Mitarbeiter verwaltet und andererseits damit klarkommt, dass von einem Tag auf den anderen das ganze Unternehmen von zu Hause aus arbeitet, ist ein sehr starkes Tool für die Geschäftskontinuität. Darüber hinaus nutzt sie die Cloud, um IT- und Sicherheitsteams die nötige Flexibilität zur Ermöglichung dieser Abläufe zu bieten. Die Wahrung der Sicherheit, Benutzerfreundlichkeit und Benutzererfahrung ist für die Benutzer von entscheidender Bedeutung, und nur wenige Lösungen können all dies gewährleisten.

Die Nutzung einer ZTNA-Lösung gegenüber einer VPN-Alternative bringt mehrere Vorteile:

- **Eliminierung oder Verringerung der teuren VPN-Nutzung:** VPN-Lösungen sind oft langsam und kompliziert. Ihnen mangelt es an Benutzerfreundlichkeit für die Mitarbeiter und können für die Betreiber aufwändig zu verwalten und kostspielig zu aktualisieren sein.
- **Sicherer Multicloud-Zugriff:** Die Sicherung des Hybrid- und Multicloud-Zugriffs ist ein guter Ausgangspunkt für Unternehmen auf ihrem ZTNA-Weg. Da immer mehr Unternehmen auf die Cloud umsteigen, entscheiden sich viele für ZTNA, um ihre Multicloud-Strategie zu ermöglichen.
- **Verringerung des Fremdnutzerrisikos.** Benutzer außerhalb des Unternehmens erhalten oft einen Zugang mit unnötigen Berechtigungen, was zu einer Sicherheitslücke führen kann. ZTNA reduziert das Risiko durch Drittnutzer erheblich, indem es sicherstellt, dass externe Benutzer nie auf das gesamte Netzwerk zugreifen und nur Zugriff auf die für sie erlaubten oder relevanten Anwendungen erhalten.

Technologieprofil

Systancia Gate ist eine Cybersicherheitslösung, die Benutzern außerhalb des Unternehmensnetzwerks, z. B. Remote-Benutzern, Heimarbeitern und Drittanbietern, sicheren Zugriff auf Unternehmensressourcen und -anwendungen bietet. Es bietet eine Zugriffsarchitektur, die nur ausgehende Datenströme und keine Portöffnung zum IT-System umfasst, und wird hauptsächlich von Unternehmen und Serviceanbietern verwendet, um einen sicheren Zugriff auf Unternehmensanwendungen zu gewährleisten.

Die Lösung basiert auf dem ZTNA-Prinzip und ermöglicht fein abgestimmte Benutzerzugriffsprofile, die nicht das gesamte Netzwerk, sondern spezifische IT-Ressourcen und -Anwendungen zugänglich machen. Sie ermöglicht es Unternehmen, jeden beliebigen Endpunkt oder jedes Endgerät einschließlich PCs für den Zugriff auf IT-Ressourcen und -Anwendungen über das Netzwerk zu nutzen. Dabei gelten strenge Zugriffsregeln, je nachdem, wer darauf zugreift und worauf zugegriffen wird – beispielsweise Behörden oder Krankenhäuser. Das wäre mit dem traditionelleren Ansatz einer VPN-Lösung nicht möglich. Systancia Gate kann die Mobilität der Mitarbeiter fördern, da Mitarbeiter von überall innerhalb und außerhalb der Unternehmensnetzwerke arbeiten und sofortigen Zugriff auf Arbeitsumgebungen erhalten können, wobei sie in Sachen Ergonomie und Leistung die gewohnte Benutzererfahrung genießen. Die Lösung kann innerhalb weniger Stunden im Unternehmen bereitgestellt werden und bietet Mitarbeitern die gleiche Arbeitsumgebung, die sie gewohnt sind und täglich im Büro nutzen.

Sobald der sichere Remote-Zugriff über Systancia Gate für alle Mitarbeiter aktiviert ist, erhalten diese bei der Arbeit mit Systancia Workplace den nötigen Zugriff, um auf einem virtuellen Desktop arbeiten zu können und sowohl vor Ort als auch in der Cloud all ihre beruflichen Anwendungen nutzen zu können. Alle Benutzer haben Zugriff auf ihre Arbeitsumgebung, unabhängig von ihrem Standort (im Büro, auf Reisen oder zu Hause) und dem verwendeten Gerät (Workstations, Laptops, Tablets oder Smartphones).

Für die Endbenutzer arbeitet die Lösung mit einem Architekturtunnel: Auf dem Gerät ist nichts installiert, alles geschieht in einem Webbrowser, in dem sie ihre übliche Umgebung vorfinden. Alles, was sie brauchen, ist ihre Tastatur und ihre Maus. Nicht agentenbasierte Lösungen ermöglichen es Remote-Mitarbeitern, ihre Arbeit direkt von ihren eigenen persönlichen Geräten aus wiederaufzunehmen, ohne Agents oder zusätzliche Software herunterladen und installieren zu müssen. Dadurch werden die Komplexität und einige der Bedenken hinsichtlich des Datenschutzes gemindert, die sie möglicherweise haben, wenn auf ihrem PC Unternehmenssoftware aktiviert ist. Zusätzlich zur Bereitstellung des Zugriffs auf Desktops und Anwendungen können die Unternehmen mit Systancia Workplace, einem Add-on für Systancia Gate, den Benutzern auch virtuelle Desktops zur Verfügung stellen.

Die Lösung hilft den IT-Teams außerdem beim Workstation-Management und vermeidet teilweise den Aufwand, der mit der Nutzung mehrerer heterogener Produkte und punktueller Lösungen einhergeht, die nicht immer gut miteinander harmonieren. So kann dies beispielsweise in Unternehmen mit mehreren Rechenzentren auch hinsichtlich der Verwaltung ein Vorteil sein, da nur ein Zugriff benötigt wird und alle Vorgänge über ein einheitliches Managementportal ausgeführt werden. Systancia Workplace bietet den Benutzern eine einheitliche Konsole („Single Pane of Glass“), sozusagen ein einziges Fenster zu allen Anwendungen und Ressourcen, die ihrerseits in so vielen Rechenzentren wie nötig untergebracht sein können.

Warum ZTNA VPN ersetzen wird

VPN-Lösungen sind nicht auf die Remote-Arbeit in einem großen Umfang ausgelegt, wie es in den meisten Ländern während der COVID-19-Lockdowns die Regel war. Oftmals musste die gesamte Belegschaft von zu Hause aus arbeiten, und viele mussten mit ihrem eigenen PC auskommen. Die Bereitstellung von Unternehmens-VPNs auf privaten Geräten ist nicht unbedingt sicher, da die Herstellung einer VPN-Verbindung von einem nicht vertrauenswürdigen Gerät aus gefährlich sein kann und für viele Unternehmen schlicht nicht skalierbar ist. Die Ausweitung des Zugriffs über VPN auf die gesamte Belegschaft bringt auch zusätzliche Kosten mit sich, erfordert mehr IT-Kapazitäten und schafft Leistungsprobleme und Schwierigkeiten mit der Gerätekompatibilität. Außerdem muss für VPNs ein Agent auf dem Gerät des Benutzers ausgeführt und ein vom Unternehmen kontrolliertes Gerät muss betrieben werden. Mit einem VPN ist keine Überwachung/Nachverfolgung möglich: Man sieht nicht, wer worauf Zugriff hat.

Systancia Gate basiert auf einem ZTNA-Ansatz, bei dem ein softwaredefinierter Perimeter mithilfe eines Controllers eine direkte Verbindung zwischen dem Gerät eines Benutzers und nur den autorisierten Anwendungen authentifiziert und herstellt. Diese Lösungen verwenden einen Out-of-Band-Controller für Richtlinienentscheidungen und -durchsetzung (Anwendung von Zugriffsregeln/-richtlinien) sowie Gateways zur Öffnung eines Tunnels zum Controller (wobei der Tunnel vom Eingangsendpunkt des Benutzers bis zum Ausgang des Gateways reicht). Das Modell ermöglicht es dem Controller (der in der Cloud oder On-Premises implementiert sein kann), eine sichere Verbindung zwischen dem Endpunkt und der Anwendung herzustellen, wodurch ein direkter Kommunikationspfad zwischen Benutzer und Anwendung bereitgestellt wird.

Mit ZTNA bleibt das Benutzererlebnis erhalten, da keine zusätzlichen Schritte auf Benutzerseite erforderlich sind und kein Daten-Backhaul und keine Latenz gegeben sind, wie es bei einem herkömmlichen VPN der Fall wäre. Der Anwendungszugriff ist vom Netzwerkzugriff entkoppelt, sodass die Nutzer das Internet als sicheres Netzwerk nutzen können. Den Administratoren hilft ZTNA, die Aktivität zwischen Benutzern und Apps zu überwachen, jede Transaktion (z. B. in einer Finanzorganisation) zu verfolgen und identitätsbezogene Daten zu erfassen. ZTNA kann auch bei der Kostenverwaltung helfen, da sich der Preis der Angebote in der Regel nach der Anzahl der benannten Benutzer statt nach der Zahl gleichzeitiger Benutzer wie bei VPN-Lösungen richtet. Bei Systancia Gate basierte der Preis anfänglich auf der Zahl gleichzeitiger Benutzer wie bei VPN-Lösungen, doch in Krisenzeiten liegt die Anzahl gleichzeitiger Benutzer sehr nahe an der Anzahl benannter Benutzer.

Durch den Einsatz einer Lösung wie Systancia Gate gegenüber herkömmlichen Produkten für den Netzwerkzugriff, wie z. B. einem VPN, profitieren Kunden von folgenden Vorteilen:

- Zero-Trust-Zugriff auf die Anwendungen des Unternehmens über ein privates Netzwerk
- kontrollierter und selektiver Zugriff auf Infrastrukturressourcen
- verbesserte Sicherheit von mobilen Geräten mit Active Sync und OTP-Authentifizierung
- Installation nach Best Practices in Sachen Sicherheit
- adaptive Authentifizierungsfunktionen

Systancia Gate enthält auch Funktionen zur Überwachung und Überprüfung von Aktionen, die von Benutzern außerhalb des Unternehmens durchgeführt werden.

Ein weiterer Anwendungsfall, der während der COVID-19-Krise erkannt wurde, besteht darin, den Benutzern Zugriff auf ihren Büro-PC zu gewähren. Systancia Gate bietet Remote-Zugriff auf Desktops und „koppelt" den Zugriff des Benutzers automatisch mit seinem Büro-PC.

Herausforderungen

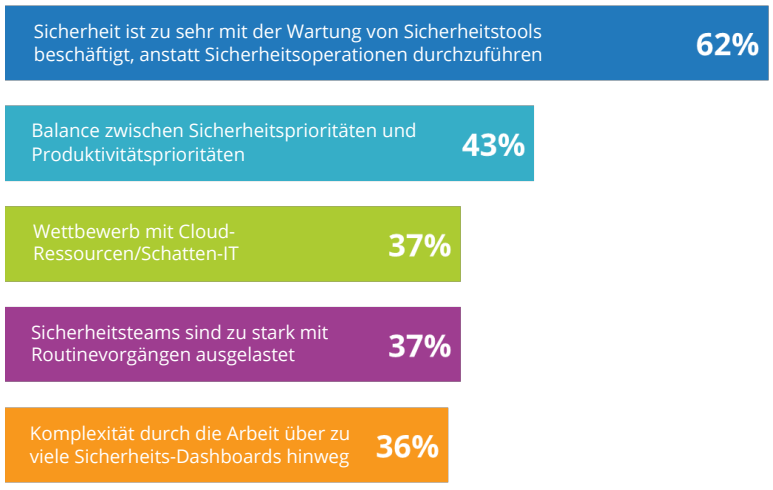
Trotz der Vorteile der ZTNA-Lösungen gegenüber dem traditionelleren VPN-Ansatz bestehen bei der Einführung solch völlig neuer Lösungen auch Herausforderungen. Sicherheitsteams fehlen unter Umständen das nötige Wissen und Selbstvertrauen, die unmittelbaren Finanzmittel oder die Genehmigung des Vorstands, um ZTNA bereitstellen zu können. Sie werden daher möglicherweise gebeten, mit ihrer bestehenden Infrastruktur weiterzuarbeiten und ihre aktuellen VPN-Produkte und -Lösungen zu erweitern.

Trends

Wenn viele unterschiedliche Sicherheitsprodukte im Einsatz sind, kann dies einen großen Verwaltungsaufwand für die IT- und Sicherheitsteams bedeuten. Die Integration aller Produkte auf einer einzigen Plattform oder einem einzigen Portal verbessert daher die Benutzerfreundlichkeit und das Anwendererlebnis. Laut der *European Security Strategies Survey* (Europäische Befragung zu Sicherheitsstrategien) von IDC ist der Unterhalt der Sicherheitstools der Hauptgrund dafür, wenn sich ein Unternehmen nicht weiterentwickeln kann. Dies zeigt, wie wichtig es ist, Lösungen zu vereinfachen und zu integrieren (siehe Abbildung 1).

Europäische Unternehmen haben außerdem Schwierigkeiten, die durch das Geschäft vorgegebenen Prioritäten Sicherheit und Produktivität unter einen Hut zu bringen. Bisweilen sind sie mit dem Alltagsbetrieb derart ausgelastet, dass sie sich nicht auf Sicherheitsstrategien konzentrieren können.

ABBILDUNG 1
Was schränkt die Fähigkeit Ihres Unternehmens ein, seine Sicherheitsfunktionen zu verbessern?



Quelle: IDC, *European Security Strategies Survey, 2019* (n = 700)

Future of Work

Sicherheit hat bei den Strategien für die Zukunft der Arbeit oberste Priorität. Es ist wichtig, sich von der Komplexität zu verabschieden, die die Verwaltung mehrerer verschiedener Plattformen mit sich bringt, und auf ein einheitlicheres und integriertes Endnutzererlebnis über alle Geräte hinweg hinzuarbeiten. Dies lässt sich durch einen Zero-Trust-Ansatz für das gesamte Unternehmen erreichen. Zero Trust und kontextbezogene Zugriffssteuerung sind Frameworks für die Implementierung von Sicherheit im Gegensatz zu einzelnen Sicherheitsprodukten und -lösungen. Zur Implementierung erfordern sie einen koordinierten Ansatz bei den Mitarbeitern, Prozessen und Technologien. Der erste Aspekt besteht darin, sich die Belegschaft anzusehen und sicherzustellen, dass jeweils nur die richtigen Benutzer und Geräte auf Netzwerke und Anwendungen zugreifen können. Man überprüft die Identität der Benutzer und kennzeichnet Geräte als vertrauenswürdig, bevor der Zugriff auf Netzwerke und Anwendungen von überall aus gewährt wird. Dadurch wird auch sichergestellt, dass Benutzer und Geräte vor Angriffen wie Phishing, Credential Stuffing und anderen identitätsbasierten Angriffen geschützt sind und dass sie die neueste Geräte-Firmware und die neuesten Anwendungsversionen ausführen.

Der zweite Aspekt betrifft den Workload-Schutz, indem alle Verbindungen innerhalb von Anwendungen über Rechenzentren und Multicloud-Umgebungen hinweg gesichert werden. Die Daten und der Datenfluss befinden sich nun außerhalb des herkömmlichen Perimeters, in der Cloud, im Internet of Things (IoT) und im Edge und sind mobil. Die Implementierung von Mikrosegmentierung hilft dabei, Sicherheitsverletzungen zu begrenzen und laterale Bewegungen zu minimieren, um tiefere Einblicke in Ereignisse über Netzwerke, Anwendungen und Server hinweg zu erhalten.

Sicherheit als Business Enabler

Unternehmen stehen im Zeitalter der DX vor neuen Herausforderungen in Bezug auf die Sicherheit. Sie sind mit großen Umwälzungen konfrontiert – für das Sicherheitsteam bietet dies die Möglichkeit, sich als Wegbereiter innerhalb des Unternehmens zu positionieren. Sicherheitsmaßnahmen können Mitarbeitern dabei helfen, jederzeit und überall sicher auf die benötigten Tools zuzugreifen und sie zu nutzen, und den sicheren Remote-Zugriff auf das Netzwerk als langfristige Strategie und nicht nur als Hauruck-Lösung zu betrachten.

Da Homeoffice zur Norm wird, kommt eine Reihe neuer Maßnahmen aufs Tapet – mittlerweile ist man sich einig, dass ein höherer Prozentsatz der Arbeitnehmer auf Dauer von zu Hause aus arbeiten wird, wobei Ideen wie Telearbeitstage an Freitagen und neue Entwicklungsbereiche für HR und Finanzen darauf abzielen, den Arbeitnehmern unabhängig vom Standort die gleiche Erfahrung zu bieten wie im Büro.

Die jüngsten Ereignisse haben gezeigt, wie wichtig es ist, einen Plan zur Aufrechterhaltung des Geschäftsbetriebs zu haben und einen Notfallplan für die Pandemieplanung in der Zukunft zu erstellen. Der Aufbau von Programmen für Cyberresilienz, die einen sicheren, skalierbaren Remote-Zugriff für die gesamte Belegschaft umfassen, um aktuell und langfristig die Geschäftskontinuität sicherzustellen, ist von entscheidender Bedeutung.

Kundenfallbeispiel: Psychiatrie und Nervenheilklinik GHU Paris

Im April 2020 wurde Systancia Gate sehr schnell – an nur einem Wochenende – in der Groupe Hospitalier Universitaire (GHU) Paris bereitgestellt und konfiguriert, sodass rund hundert Mitarbeiter aus verschiedenen Abteilungen (Personalwesen, Buchhaltung, Kommunikation usw.) ihre Aktivitäten von zu Hause aus ausführen konnten – eine Praxis, die in Krankenhäusern nicht sehr häufig vorkommt. Telearbeit im großen Maßstab darf nicht auf Kosten der IT-Sicherheit gehen. COVID-19 allein brachte das Unternehmen schon unter großen Druck, doch Krankenhäuser sind im Allgemeinen zusätzlich mit einer zunehmenden Anzahl von Cyberangriffen konfrontiert, wie Denial-of-Service-, Phishing- und Ransomware-Attacken. IT-Systeme in Krankenhäusern sind anfällig, und die Hacker haben es auf hochsensible Gesundheitsdaten abgesehen.

Nach Angaben der Klinik waren Implementierung und Benutzerschulung unkompliziert. Das doppelte Authentifizierungssystem schützt den Fernzugriff vor 90 Prozent der Standardangriffe, und die HTML5-Technologie ermöglicht Benutzern den Zugriff auf ihren Remote-Desktop über ihren Browser, wodurch die Verwendung der Lösung erleichtert wird, da keine Erweiterungen installiert werden müssen.

Die Lösung trennt außerdem die Aktionen des Benutzers auf dem Desktop von denen auf dem System, wodurch beide Bereiche voneinander abgeschottet sind. Mit Systancia Gate konnten die Krankenhausmitarbeiter – ob auf dem eigenen PC oder anders – von zu Hause aus arbeiten, während der Schutz der IT-Systeme der Klinik gewährleistet war.

Fazit

Unternehmen müssen ihren Mitarbeitern überall und jederzeit dieselbe Arbeitsumgebung, die gleiche Performance und die gleiche Benutzererfahrung bieten wie im Büro – und das auf sichere Weise.

ZTNA-Lösungen wie Systancia Gate bieten den Benutzern einen Mehrwert und werden über die Cloud verwaltet. Zu ihren Vorteilen zählen Flexibilität, Agilität und die Nachhaltigkeit der Lösungen, mit deren Hilfe Unternehmen schneller die nötigen Zugriffsmechanismen für die „neue Normalität" der Remote-Arbeit umsetzen können. Wenn wir COVID-19 bewältigt haben, werden Führungskräfte, Kollegen und Mitarbeiter vielleicht wieder im Büro arbeiten oder auch nicht – jedenfalls wohl kaum genauso wie zuvor. Die Zunahme der Anzahl von Menschen, die von zu Hause aus arbeiten, bringt es allerdings mit sich, dass sich die Art und Weise, wie wir arbeiten, für immer verändern wird. Nach dem durch COVID-19 ausgelösten massenhaften Umstieg auf das Homeoffice dürfte sich der IT eine Neubewertung ihres Ansatzes bezüglich der Mitarbeiter, deren Authentifizierung und Fernzugriff aufdrängen. VPNs werden sich in den kommenden Jahren wahrscheinlich einer stärkeren Konkurrenz durch ZTNA-Lösungen gegenübersehen. COVID-19 hat den Bedarf an Technologien für den Remotezugriff einschließlich VPN-Produkten deutlich gemacht, doch die vielen neuen Anwendungsfälle für das Homeoffice sind für ältere VPN-Ansätze eine Herausforderung, da es erforderlich ist, neue Appliances einzukaufen, ausliefern zu lassen und bereitzustellen sowie Software für die Endpunkte bereitzustellen.

Die Kunden halten zunehmend nach alternativen Lösungen Ausschau, die einen sicheren Remote-Zugriff ermöglichen und sich gleichzeitig an den Konzepten der verteilten Integrität und des digitalen Vertrauens orientieren. Sie bitten ihre MSPs und CSPs, ZTNA-Lösungen anzubieten, damit sie diese in ihren eigenen Unternehmen einsetzen können.

Über den Analysten

Romain Fouchereau, Research Manager, IDC European Security

Als Research Manager der European Security Research Group konzentriert sich Romain Fouchereau besonders auf Sicherheits-Appliances, Netzwerksicherheit und IoT-Sicherheit. Er leitet außerdem die European IT/OT Convergence Practice von IDC.

Über IDC

International Data Corporation (IDC) ist der weltweit führende Anbieter von Marktinformationen, Beratungsdienstleistungen und Veranstaltungen auf dem Gebiet der Informations- und Verbrauchertechnologie und der Telekommunikation. IDC analysiert und prognostiziert technologische und branchenbezogene Trends und Potenziale und ermöglicht seinen Kunden so eine fundierte Planung ihrer Geschäftsstrategien sowie ihres IT-Einkaufs. Mehr als 1.100 IDC-Analysten in über 110 Ländern liefern globale, regionale und lokale Erkenntnisse zu technologie- und branchenbezogenen Chancen und Trends. Seit 50 Jahren vertrauen Business-Verantwortliche und IT-Führungskräfte bei der Entscheidungsfindung auf IDC. IDC ist ein Geschäftsbereich der IDG, dem weltweit führenden Unternehmen in den Bereichen IT-Publikationen, Research sowie Ausstellungen und Konferenzen.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
+44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Hauptsitz

5 Speen Street, Framingham, MA
01701 USA
Tel.: 508-872-8200
Fax: 508-935-4015
www.idc.com

Copyright und Einschränkungen