Whitepaper

Mehr Produktivität für hybride Belegschaften durch optimierte Sicherheit und User Experience

Einführung

In Zukunft wird hybrid gearbeitet. Die vergangenen drei Jahre standen bei vielen Organisationen ganz im Zeichen der rapiden Umstellung auf neue Tools und Technologien zur Unterstützung von Remote-Arbeit. Mittlerweile setzt sich allerdings immer mehr die Erkenntnis durch, dass beide Modelle — Remote- und Präsenzarbeit — jeweils eigene Vor- und Nachteile haben. Infolge des plötzlichen Umzugs vieler Mitarbeiter ins Homeoffice wurde vielen Führungskräften der Wert persönlicher Interaktionen zur Stärkung von Teamgeist und Unternehmenskultur überhaupt erst bewusst. Dem gegenüber stand die Feststellung, dass Mitarbeiter im Homeoffice außerordentlich produktiv sein können und ihrerseits die Flexibilität und ausgewogene Work/Life-Balance der Remote-Arbeit zu schätzen wissen.

Im Bestreben, von den Vorteilen beider Modelle zu profitieren, holen viele Unternehmen ihre Angestellten wenigstens für einen bestimmten Teil der vereinbarten Arbeitszeiten wieder zurück ins Büro. Dabei gewähren sie ihnen jedoch ein sehr hohes Maß an Flexibilität.

Eine überwältigende Mehrheit von 77 % der Unternehmen hat bereits auf hybride Arbeitsmodelle umgestellt. Am beliebtesten sind flexible Konzepte, bei denen die Mitarbeiter selbst entscheiden können, an welchen Tagen sie im Büro arbeiten wollen. Dieses Modell hat den großen Vorteil, dass es Mitarbeitern sehr viel Flexibilität ermöglicht, die wiederum zu höherer Zufriedenheit und in vielen Fällen auch zu mehr Produktivität führt.

Trotz der global anhaltenden wirtschaftlichen Ungewissheit ist der Arbeitskräftemarkt aktuell so angespannt wie selten zuvor in der Geschichte. In den USA stehen für über zehn Millionen offene Stellen derzeit nur sechs Millionen Arbeitssuchende zur Verfügung, wie eine Studie der US-Handelskammer ergab. Entsprechend haben Unternehmen aller Größen und Branchen Schwierigkeiten, Positionen auf sämtlichen Ebenen von Einstiegsjobs bis zur Chefetage zu besetzen.

Angesichts des akuten Fachkräftemangels ist es für Organisationen absolut unerlässlich, Technologie-gestützte Optionen anzubieten, die zur Steigerung der Zufriedenheit und Produktivität ihrer Mitarbeiter beitragen und ihnen gleichermaßen zuverlässige Unterstützung bei der Präsenzarbeit an Unternehmensstandorten wie auch im Homeoffice oder unterwegs leisten.

Trotzdem haben viele Organisationen bislang noch keine langfristige Strategie erarbeitet um zu gewährleisten, dass sämtliche Mitarbeiter standortunabhängig auf alle Anwendungen zugreifen können, die sie zur Erledigung ihrer Aufgaben benötigen. Nur durch eine derartige Strategie lässt sich ein nahtloser und sicherer Zugriff mit hervorragender User Experience auf Anwendungen ermöglichen, die teils in Cloud-Umgebungen, teils im privaten Rechenzentrum des Unternehmens gehostet werden.

Hier sind neue Lösungen gefragt, die hervorragende Anwendererfahrungen gewährleisten und gleichzeitig zuverlässigen Schutz vor Cybersicherheitsrisiken bieten. Aktuell arbeiten viele Organisationen an der Entwicklung langfristiger Strategien und Arbeitsmodelle. Damit gewinnt auch die Notwendigkeit an Bedeutung, Usern in Präsenz- und Remote-Arbeit ein identisch hohes Schutzniveau bei gleichermaßen hervorragenden Anwendererfahrungen bereitzustellen. Insbesondere gilt dies auch für Szenarien, in denen Mitarbeiter flexibel zwischen Unternehmensstandorten und Homeoffice hin und her wechseln.

Welche Voraussetzungen müssen zum Schutz hybrider Belegschaften erfüllt sein?

Traditionell herrschte unter Technologiebeauftragten die Ansicht vor, robuste Sicherheit und einfacher Zugriff auf Ressourcen seien zwei wünschenswerte Ziele, die sich leider gegenseitig ausschließen. Heute sind cloudbasierte Lösungen erhältlich, die Usern schnellen, reibungslosen Zugriff auf alle erforderlichen Anwendungen gewährleisten, ohne die Sicherheit zu beeinträchtigen. Zudem können IT-Verantwortliche für alle Mitarbeiter völlig unabhängig vom jeweiligen Standort ständigen Bedrohungsschutz und Konnektivität mit geringer Latenzzeit ermöglichen.

Mithilfe dieser Lösungen erfüllen Organisationen die beiden wichtigsten Voraussetzungen für eine erfolgreiche Umstellung auf Hybridarbeit, da sie sowohl **Sicherheit** als auch **hochwertige Anwendererfahrungen gewährleisten**. Was das konkret bedeutet, wird im Folgenden erläutert.

User Experience

Herkömmliche Hub-and-Spoke-Netzwerke sind nicht darauf ausgelegt, die Ansprüche hybrider Belegschaften zu erfüllen — geschweige denn, ihre Produktivität zu steigern. In Netzwerken, die nach diesem Modell aufgebaut sind, werden Sicherheitsrichtlinien durch Appliances und Firewalls im Rechenzentrum des Unternehmens durchgesetzt. Entsprechend muss der gesamte Traffic über diesen Security-Stack geroutet werden. Dieses Backhauling des Traffics verlangsamt die Anwendungsleistung, was angesichts der zunehmenden Bedeutung von Videokonferenzsoftware und anderen latenzanfälligen Kooperationstools im Arbeitsalltag besonders problematisch ist.

Mit herkömmlichen Sicherheitsarchitekturen ist kein reibungsloser Remotezugriff auf Unternehmensressourcen möglich. Stattdessen müssen umständliche Behelfslösungen wie virtuelle private Netzwerke (VPNs) mit komplexen Anmeldevorgängen eingerichtet werden. Unvermeidliche Folge ist, dass sich die Verfahren, mit denen Remote-Mitarbeiter auf geschäftskritische Anwendungen und andere Ressourcen zugreifen, grundlegend von den gewohnten Arbeitsabläufen im Büro unterscheiden.

Angesichts zunehmend verteilter Belegschaften wird es für IT-Teams auch immer schwieriger, Probleme zu verfolgen und zu lösen, die sich auf Enduser auswirken. Bisherige Tools für die Überwachung von Geräten, Netzwerk und Anwendungen gewährleisten keine lückenlosen Einblicke in die gesamte Bereitstellungsumgebung. Infolgedessen entstehen Transparenzlücken im Verbindungspfad zwischen Endgerät und Anwendung. Um diese Lücken zu schließen, müssen IT- und Servicedesk-Mitarbeiter Daten aus unterschiedlichen Tools manuell exportieren und korrelieren. Dadurch werden IT-Teams dauernd in die Defensive getrieben: Anstatt Probleme proaktiv zu erkennen und zu beheben, bevor sie die Produktivität der User beeinträchtigen, betreiben sie nachträgliche Schadensbegrenzung und Brandbekämpfung.

Für ein effektiveres Arbeiten sind Lösungen erforderlich, die standortunabhängig zügigen, reibungslosen Zugriff auf das Internet sowie auf interne und SaaS-Anwendungen gewährleisten, damit alle Mitarbeiter jederzeit von optimalen Anwendererfahrungen profitieren. In technischer Hinsicht lässt sich dies am besten durch ein direktes Peering erreichen, um User immer auf dem kürzesten Pfad mit der jeweils erforderlichen Anwendung zu verbinden. Durch direktes Peering werden Latenzzeiten dramatisch reduziert, da die Weiterleitung über VPNs und Firewalls entfällt.

Zudem werden Lösungen benötigt, die IT-Fachkräfte in die Lage versetzen, die Performance von Anwendungen aus der Perspektive der Enduser in Echtzeit zu überwachen. Dadurch lassen sich etwaige Probleme proaktiv beheben, bevor sie den Usern überhaupt auffallen.

Sicherheit

Die weit verbreitete Umstellung auf Remote-Arbeit hat zu einer enormen Vergrößerung der Angriffsfläche geführt. Das liegt vor allem daran, dass viele neue Geräte mit Unternehmensnetzwerken verbunden werden, um auf Ressourcen zuzugreifen. Bedrohungsakteure nehmen mit Vorliebe überlastete VPNs und Firewalls ins Visier und suchen nach Möglichkeiten, deren begrenzte Schutzmechanismen zu umgehen. Gelingt ihnen dies, haben sie vollen Zugriff auf das Netzwerk und alle darin gespeicherten Ressourcen. Entsprechend hoch ist das Risiko, dass wertvolle vertrauliche Daten offengelegt oder gestohlen werden.

Wer Sicherheitsverletzungen in den komplexen IT-Ökosystemen heutiger Organisationen effektiv verhindern will, muss sich von der Vorstellung verabschieden, Usern Zugriff auf das gesamte Netzwerk zu gewähren. Stattdessen dürfen sie nur nach Bedarf auf einzelne Anwendungen zugreifen. Dies entspricht dem Grundsatz der Mikrosegmentierung, einem Kernkonzept des Zero-Trust-Sicherheitsansatzes. Durch Einhaltung dieses Prinzips wird zum einen das Risiko lateraler Bewegungen innerhalb des Netzwerks minimiert,

sodass Bedrohungsakteure ein einziges infiziertes Konto nicht als Sprungbrett für den Zugriff auf andere Unternehmensressourcen missbrauchen können. Zum anderen wird verhindert, dass Anwendungen im öffentlichen Internet sichtbar sind. Dadurch wird die Angriffsfläche der Organisation radikal verkleinert.

Legacy-Firewalls sind nicht in der Lage, Bedrohungen in verschlüsseltem Traffic zu erkennen. Mittlerweile wird jedoch ein Großteil aller Malware-Angriffe im verschlüsselten Traffic versteckt. Ein neuer Ansatz, der den gesamten Traffic unabhängig vom Ursprung und Ziel untersuchen kann, ist daher eine unverzichtbare Voraussetzung für einen effektiven Schutz von Daten. Dabei muss sowohl Traffic von und zu Geräten berücksichtigt werden, die vom Unternehmen verwaltet werden, als auch von und zu Eigengräten der Mitarbeiter.

Zudem werden neue Lösungen benötigt, die eine reibungslose Durchsetzung konsistenter Datenschutzrichtlinien selbst in komplexen dezentralen Umgebungen ermöglichen.

Die Zscaler Zero Trust Exchange: Universal Zero Trust Network Access für Anwendungen und User unabhängig vom Standort

Immer mehr Organisationen stellen zum Schutz hybrider Belegschaften auf Zero-Trust-Konzepte um. Zscaler hat die Zero Trust Exchange speziell als eine unternehmensfähige Sicherheitslösung entwickelt, die Organisationen dabei unterstützen soll, ihren Mitarbeitern sicheren Zugriff auf alle benötigten Anwendungen zu ermöglichen. Die Zero Trust Exchange setzt das Prinzip der minimalen Rechtevergabe durch und gewährleistet, dass User und Anwendungen niemals inhärent als vertrauenswürdig eingestuft werden. Alle beschriebenen Funktionen werden über eine einzige Plattform bereitgestellt, die sämtliche Kommunikationen zwischen Usern, Workloads und Geräten unabhängig vom Netzwerk und Standort absichert.

ZTNA zum Schutz hybrider Belegschaften

Zur Unterstützung des anhaltenden Trends zu Hybrid- und Remote-Arbeit sind Technologien erforderlich, die die dadurch entstehenden Sicherheitsrisiken minimieren. Vor diesem Hintergrund hat sich das Konzept des Zero Trust Network Access (ZTNA) in den vergangenen Jahren zunehmend durchgesetzt. Das Konzept stammt ursprünglich von der Analystenfirma Gartner und sieht die Einrichtung einer identitäts- und kontextbasierten, durch technische Zugriffskontrollen gesicherten Schutzgrenze um unternehmenseigene Anwendungen und Ressourcen vor. Um diese Schutzgrenze durchzusetzen, vermitteln ZTNA-Services Verbindungen zwischen befugten Usern und den jeweils benötigten Anwendungen. Zugriffsanforderungen werden nur in Übereinstimmung mit Zero-Trust-basierten Sicherheitsrichtlinien genehmigt.

ZTNA ist indes mehr als nur eine effektivere Alternative zu VPNs. Der eigentliche Vorteil dieses Konzepts liegt darin, dass es sich gleichermaßen für User in Präsenzarbeit wie an Remote-Standorten empfiehlt. Universal ZTNA bedeutet, dass User standortunabhängig — also im Homeoffice ebenso wie in der Unternehmenszentrale — von identischem Zugriffsschutz auf Zero-Trust-Basis profitieren.

Als Universal ZTNA wird die Erweiterung von ZTNA-Funktionen bezeichnet, sodass sie für Mitarbeiter an Unternehmensstandorten ebenso reibungslos funktionieren wie für Remote-User. Dabei muss gewährleistet sein, dass beide Gruppen von identischen Anwendererfahrungen und Sicherheitsfunktionen profitieren. Eine entsprechende Lösung muss in der Lage sein, sowohl sichere Direktverbindungen zu Anwendungen in der Cloud als auch Verbindungen für lokale User bereitzustellen, die auf Anwendungen im Rechenzentrum des Unternehmens zugreifen.

Als Cloud-native Plattform vermittelt die Zero Trust Exchange schnelle und sichere Verbindungen zum Internet, privaten Unternehmensanwendungen und SaaS-Umgebungen. User und Administratoren profitieren dabei sowohl in der Unternehmenszentrale als auch in allen Zweigstellen und an Remote-Standorten von optimalen Anwendererfahrungen. Die Zero Trust Exchange ist darauf ausgelegt, ein hohes Schutzniveau ohne Beeinträchtigung der User Experience zu gewährleisten. Ihre Bereitstellung bietet Organisationen eine ganze Reihe von Vorteilen:

- Schneller, nahtloser Zugriff von überall: Die Zero Trust Exchange gewährleistet, dass der Traffic immer auf dem kürzesten Verbindungspfad zwischen Usern und Zugriffszielen geroutet wird. Zscaler-Kunden profitieren dabei von Peering-Vereinbarungen mit SaaS-Anbietern und Zugriff über einen Broker in unmittelbarer User-Nähe. Die Bereitstellung von VPNs und Firewalls wird ebenfalls überflüssig.
- Geringere Risiken für das Unternehmen: Durch Direktzugriff auf Anwendungen wird Mikrosegmentierung durchgesetzt. Die Zero Trust Exchange stellt auf Einzelfallbasis Verbindungen zwischen Usern und den jeweils benötigten Anwendungen her, um die Angriffsfläche zu verkleinern. Im Falle einer Kompromittierung einzelner User-Konten können Bedrohungen sich nicht innerhalb des Netzwerks verbreiten.
- Herausragende digitale Anwendererfahrungen: Mit der Zero Trust Exchange können IT-Beauftragte die Performance von Anwendungen aus der Perspektive der Enduser überwachen. Etwaige Probleme mit Anwendungen, Netzwerken und Geräten lassen sich dadurch frühzeitig beheben, bevor sie die Produktivität der User beeinträchtigen.

Mit der Einführung von Zscaler Private Access (ZPA) Private Service Edge erfüllt die Zscaler Zero Trust Exchange sämtliche Ansprüche an die Bereitstellung von Universal ZTNA. Mit ZPA Private Service Edge profitieren Organisationen jetzt auch zum Schutz privater Unternehmensanwendungen im Rechenzentrum von allen Vorteilen der Zscaler Zero Trust Exchange. Durch Bereitstellung des gesamten Funktionsumfangs der Zero Trust Exchange für private Rechenzentren und öffentliche Cloud-Edges reduziert ZPA Private Service Edge Latenzen und optimiert die Performance von Anwendungen für User an Unternehmensstandorten. Zero-Trust-Sicherheitsrichtlinien werden mit ZPA Private Service Edge möglichst nahe an der Edge durchgesetzt, um gleichermaßen hervorragende Anwendererfahrungen für alle User zu gewährleisten, die an Unternehmens- oder Remote-Standorten auf Anwendungen im Rechenzentrum oder in der Cloud zugreifen.

Mit der Zscaler Zero Trust Exchange können Organisationen echten Zero-Trust-Schutz gewährleisten, und zwar auf eine kostengünstige und effiziente Weise, die das gesamte Spektrum der Sicherheits- und Leistungsanforderungen hybrider Belegschaften erfüllt.

zscaler™ | Experience your world, secured.™

Über Zscaler
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die SSE-basierte Zero Trust Exchange ist auf über 150 Rechenzentren der ganzen Welt verteilt und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf **zscaler.de** oder folgen Sie uns auf Twitter unter **@zscaler**.

+1 408 533 0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA zscaler.de