Status der Zero-Trust-Transformation 2023

VON DER PRÄVENTION BIS ZUM ENABLEMENT:
das volle Potenzial von Zero Trust für mobile und Cloud-zentrierte Unternehmen

Inhaltsverzeichnis

Kurzfassung

Nathan Howe | VP, Emerging Technology & 5G, Zscaler

Angesichts der rasanten digitalen Transformation hat sich Zero Trust als ideales Framework für die Absicherung von geschäftlichen Usern, Workloads und Geräten in einer hochgradig verteilten, mobilen und Cloud-zentrierten Unternehmenslandschaft etabliert und revolutioniert jahrzehntelang geltende Sicherheits- und Netzwerkprinzipien.

Auch IT-Verantwortliche auf der ganzen Welt werden sich dieser Entwicklung bewusst:

Mehr als 90 % der IT-Führungskräfte, die mit dem Umstieg auf die Cloud begonnen haben, haben bereits eine Zero-Trust-Sicherheitsstrategie implementiert oder planen, eine solche innerhalb des nächsten Jahres einzuführen. Das geht aus unserer aktuellsten weltweiten Umfrage hervor, für die wir mehr als 1.900 CIOs, CISOs, CDOs, CTOs und Leiter von Infrastrukturabteilungen verschiedener Organisationen befragt haben, die bereits mit der Migration von Anwendungen und Services in die Cloud begonnen haben.

Diese Daten lassen bereits auf einen positiven Trend schließen und auch die Gründe für diese Entwicklung deuten auf eine optimistische Einstellung gegenüber der Implementierung einer Zero-Trust-Architektur hin — auch über die nächsten 12 Monate hinaus.

22 %

Da jedoch nur 22 % der Befragten davon überzeugt sind, dass ihre Organisation das gesamte Potenzial ihrer Cloud-Infrastruktur ausschöpft, deuten die Ergebnisse darauf hin, dass in Zukunft mehr als nur bloße Sicherheitsaspekte berücksichtigt werden müssen.

In der Tat scheint das Sicherheitspotenzial einer Zero-Trust-Architektur angesichts der fortschreitenden Cloud-Migration eindeutig zu sein. Mehr als zwei Drittel (68 %) der IT-Führungskräfte sind entweder der Meinung, dass eine sichere Cloud-Transformation mit der bestehenden Infrastruktur für Netzwerksicherheit nicht möglich ist oder dass Zero Trust Network Access eindeutige Vorteile gegenüber herkömmlichen Firewalls und VPNs bietet, wenn sicherer Remotezugriff auf Anwendungen bereitgestellt werden soll.

Da jedoch nur 22 % der Befragten davon überzeugt sind, dass ihre Organisation das gesamte Potenzial ihrer Cloud-Infrastruktur ausschöpft, deuten die Ergebnisse darauf hin, dass in Zukunft mehr als nur bloße Sicherheitsaspekte berücksichtigt werden müssen. Aus einer ganzheitlichen IT-Perspektive betrachtet, bietet ein Zero-Trust-Konzept im gesamten Digitalisierungsprozess zahlreiche vielversprechende Optionen — natürlich können Sie mit Zero Trust umfangreiche Cyberangriffe verhindern, doch hinter diesem Ansatz steckt noch so viel mehr: Fördern Sie die Innovationskraft in Ihrer Organisation, unterstützen Sie das Engagement Ihrer Mitarbeiter und profitieren Sie von deutlich niedrigeren Kosten.

Während sich Organisationen mit der Bereitstellung einer neuen Generation moderner Arbeitsumgebungen auseinandersetzen — hybride Modelle mit einer Vielzahl von aufkommenden Technologien wie IoT/Betriebstechnologie, 5G und sogar dem Metaverse — müssen sie ihre Sichtweise auf Zero Trust und die digitale Transformation grundlegend ändern. Mit einer Zero-Trust-Plattform lassen sich nicht nur die Anforderungen an geschäftliche und organisatorische Infrastrukturen neu gestalten: Zero Trust entwickelt sich zu einem echten Geschäftsfaktor. Mit einem solchen Ansatz können Sie hybride Arbeitsmodelle realisieren und letztlich eine moderne, vollständig digitalisierte Organisation werden — mit sämtlichen damit einhergehenden Vorteilen, von Agilität und Effizienz bis hin zu einer zukunftssicheren Infrastruktur.

Wir haben diese Studie in Auftrag gegeben, um den aktuellen Stand der Zero-Trust-Transformation in Organisationen zu ermitteln. Die Ergebnisse sind vielversprechend, denn die Implementierungsraten sind hoch. Jedoch könnten die Gründe für eine solche Implementierung durchaus ambitionierter sein. IT-Verantwortlichen bietet sich die unglaubliche Gelegenheit, die Entscheidungsträger in ihren Organisationen über Zero Trust aufzuklären und das Konzept als entscheidenden Geschäftsfaktor zu positionieren — als letztes fehlendes Element, mit dem sich Organisationen noch heute zukünftigen Technologien öffnen und mit dem sie sich auf eine erfolgreiche Zukunft vorbereiten könnten..

STATUS DER ZERO-TRUST-TRANSFORMATION

90 % Mehr als 90 % der Organisationen, die mit dem Umstieg auf die Cloud begonnen haben, haben bereits eine Zero-Trust-Sicherheitsstrategie implementiert oder planen, eine solche innerhalb der nächsten zwölf Monate einzuführen.

88 % Weltweit sind sich 88 % der IT-Führungskräfte nur zum Teil sicher, dass ihre Organisation das Potenzial der Cloud-Infrastruktur ausschöpft. Lediglich 22 % sind voll und ganz davon überzeugt.

IN DEN UNTERSUCHTEN LÄNDERN SEHEN DIE DATEN ZUR VOLLEN AUSSCHÖPFUNG DES POTENZIALS DER CLOUD-INFRASTRUKTUR FOLGENDERMASSEN AUS:

Nr. 1 Im Bereich Zero-Trust-Technologie werden Organisationen in den nächsten zwölf Monaten vor allem in ZTNA investieren — ein Hinweis darauf, wie wichtig Remotezugriff für hybride Arbeitskonzepte ist.

68 % Mehr als zwei Drittel (68 %) der IT-Führungskräfte sind entweder der Meinung, dass eine sichere Cloud-Transformation mit der bestehenden Netzwerksicherheitsinfrastruktur nicht möglich ist, oder dass Zero Trust Network Access (ZTNA) eindeutige Vorteile gegenüber herkömmlichen Firewalls und VPNs bietet, wenn sicherer Remotezugriff auf Anwendungen bereitgestellt werden soll.

54 % der IT-Führungskräfte gaben an, dass sie ihre Organisationen mit VPNs oder Perimeter-Firewalls nicht effizient vor Cyberangriffen schützen können und keine Transparenz über Anwendungstraffic und Angriffe besteht.

DIE HAUPTGRÜNDE, DIE ORGANISATIONEN DARAN HINDERN, DAS POTENZIAL DER CLOUD VOLL AUSZUSCHÖPFEN:

45 % Herausforderungen bei der Absicherung von Daten in der Cloud und Bedenken hinsichtlich des Datenschutzes

42 % Komplexe Netzwerke und schwer skalierbare Sicherheitshardware

40 % Zugriff für externe User und Remotezugriff auf IoT/Betriebstechnologie

33 % Inkonsistente Konnektivität und schlechte Anwendererfahrung beim Remotezugriff

ABGESEHEN VON SICHERHEIT, ZUGRIFF UND KOMPLEXITÄT SIND DIE WICHTIGSTEN GRÜNDE FÜR DIE IMPLEMENTIERUNG EINER ZERO-TRUST-ARCHITEKTUR NICHT AUF STRATEGISCHE GESCHÄFTSFAKTOREN ZURÜCKZUFÜHREN:

65 % Optimierte Erkennung von komplexen Bedrohungen oder Angriffen auf Webanwendungen und erhöhte Sicherheit für sensible Daten

44 % Sicherer Remotezugriff für Anbieter, Partner und Betriebstechnologie

27 % Verbesserte sichere Konnektivität für hybride Mitarbeiter

24 % Geringere Kosten und Komplexität als bei Legacy-Netzwerksicherheit

Abschnitt I

Die Cloud als wichtiger Rahmenfaktor der Zero-Trust-Einführung

Wenn wir in dieser Studie von der „Cloud“ sprechen, sind damit Anwendungen, Daten und Workloads gemeint, die als gehostete Services über das Internet und nicht in einem lokalen Rechenzentrum innerhalb eines Unternehmensnetzwerks bereitgestellt werden. Beispiele hierfür sind Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) oder private Anwendungen, die in die Cloud integriert oder dort gehostet werden.

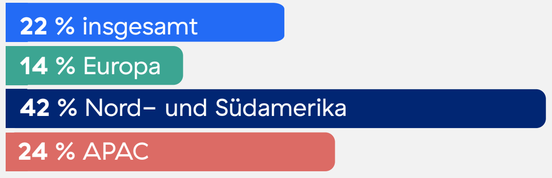
Bevor wir uns mit den konkreten Merkmalen von Zero Trust befassen, möchten wir zunächst den relevanten Kontext abstecken. Dazu sehen wir uns die gesamte IT-Landschaft genauer an und beschäftigen uns zudem damit, an welchem Punkt der Cloud-Nutzung sich Organisationen überhaupt befinden.

Zweifelsohne haben die Ereignisse der letzten Jahre dazu geführt, dass Organisationen deutlich schneller auf die Cloud umgestiegen sind. In vielen Organisationen ist der Prozess bereits weit fortgeschritten — wenn nicht sogar schon abgeschlossen.

Wir haben weltweit über 1.900 CIOs, CISOs, CDOs, CTOs und Leiter der Infrastrukturabteilungen von Organisationen befragt, die bereits mit der Migration von Anwendungen und Services in die Cloud begonnen haben. Fast die Hälfte (46 %) gab an, dass der Migrationsprozess zu 100 % abgeschlossen sei.

Doch während sich 88 % der IT-Führungskräfte zwar zum Teil sicher sind, dass sie auf dem Weg sind, die Cloud optimal zu nutzen, sind lediglich 22 % voll und ganz davon überzeugt, dass ihre Organisation das Potenzial der Cloud-Infrastruktur bereits voll ausschöpft.

UMFRAGETEILNEHMER, DIE DAVON ÜBERZEUGT SIND, DASS IHRE ORGANISATION DAS POTENZIAL DER CLOUD-INFRASTRUKTUR BEREITS VOLL AUSSCHÖPFT:



% DER BEFRAGTEN SIND DAVON ÜBERZEUGT, DASS IHRE ORGANISATION DAS VOLLE POTENZIAL DER CLOUD-INFRASTRUKTUR BEREITS AUSSCHÖPFT

Bewegen Sie den Mauszeiger auf die einzelnen Länder, um mehr zu erfahren.

Europa:

- 9 % Deutschland
- 11 % Frankreich
- 11 % Spanien
- 19 % Vereinigtes Königreich

Nord- und Südamerika:

- 41 % USA
- 51 % Brasilien

APAC:

- 16 % Singapur
- 55 % Indien

Bei der Untersuchung der regionalen Unterschiede fällt auf, dass europäische IT-Verantwortliche die stärksten Zweifel an der Nutzung ihrer Cloud-Infrastrukturen haben: Nur 14 % waren voll und ganz überzeugt, diese optimal einzusetzen. In Nord- und Südamerika liegt diese Zahl hingegen bei 42 %.

Auch wenn es keine eindeutige Ursache für diese Diskrepanz gibt, könnte ein möglicher Grund in den interkulturellen Unterschieden bei der Einführung innovativer Technologien liegen. Europäische Organisationen gehen traditionell etwas langsamer und damit vorsichtiger vor und widmen zudem dem Thema Datenschutz mehr Aufmerksamkeit. Des Weiteren verfügt Europa über eine gut ausgebaute Konnektivitätsinfrastruktur und legt seinen Fokus vor allem auf die Fertigung. Dadurch ergeben sich weniger Anreize, innovative Technologien wie 5G umgehend einzuführen, und es braucht längere Vorlaufzeiten, um etablierte Geschäftsprozesse zu ändern. Wie wir später noch näher erläutern werden, legen Organisationen in Nord- und Südamerika ihren Schwerpunkt eher auf aufkommende Technologien wie künstliche Intelligenz, maschinelles Lernen und Augmented Reality, was darauf hindeutet, dass es bereits Konzepte für Cloud-Infrastrukturen zur Unterstützung anspruchsvollerer Anwendungsfälle gibt.

Aber ganz allgemein: Warum haben Organisationen Schwierigkeiten, das volle Potenzial der Cloud auszuschöpfen?

Oberflächlich betrachtet scheint die Sicherheit das Haupthindernis zu sein, da die IT-Verantwortlichen bei der Beantwortung dieser Frage zwei sicherheitsbezogene Gründe anführten:

DIE HAUPTGRÜNDE, DIE ORGANISATIONEN DARAN HINDERN, DAS POTENZIAL DER CLOUD VOLL AUSZUSCHÖPFEN:

45 % Herausforderungen bei der Absicherung von Daten in der Cloud und Bedenken hinsichtlich des Datenschutzes

42 % Anpassung des Netzwerks zu komplex und schwer skalierbare Netzwerksicherheit

40 % Herausforderungen in Hinblick auf Zugriff für externe User und Remotezugriff auf IoT/Betriebstechnologie

33 % Inkonsistente Konnektivität und schlechte Anwendererfahrung beim Remotezugriff

DIE HAUPTGRÜNDE, DIE ORGANISATIONEN DARAN HINDERN, DAS POTENZIAL DER CLOUD VOLL AUSZUSCHÖPFEN, NACH LAND

Bewegen Sie den Mauszeiger auf die einzelnen Länder, um mehr zu erfahren.

In Europa und APAC sind Bedenken hinsichtlich des Datenschutzes das Hauptthema:

- 36 % Spanien
- 34 % Indien
- 33 % Italien
- 32 % Australien
- 28 % Frankreich

In Nord- und Südamerika geht es vor allem um die Absicherung von Daten in der Cloud:

- 44 % Brasilien
- 30 % USA

Unterdessen stießen insbesondere Singapur und Japan auf Probleme mit der Skalierung der Netzwerksicherheitshardware:

- 41 % Singapur
- 30 % Japan

In einer cloudbasierten Umgebung vergrößert sich die Angriffsfläche exponentiell, da jeder mit dem Internet verbundene Service, jeder User und jedes Gerät zu einem potenziellen Eintrittspunkt wird, einem angreifbaren Zugang zum Netzwerk, der vor Bedrohungen geschützt werden muss.

Organisationen haben berechtigte Gründe, sich Sorgen zu machen. In einer cloudbasierten Umgebung vergrößert sich die Angriffsfläche exponentiell, da jeder mit dem Internet verbundene Service, jeder User und jedes Gerät zu einem potenziellen Eintrittspunkt wird, einem angreifbaren Zugang zum Netzwerk, der vor Bedrohungen geschützt werden muss. Mehr dazu erfahren Sie im nächsten Abschnitt.

Ein Blick auf die allgemeinen Beweggründe der IT-Verantwortlichen für Cloud-Migrationen deutet jedoch auf ein viel grundlegenderes Hindernis hin — und zwar eines, das sich zweifellos auf die effektive Nutzung auswirkt. Als sie gefragt wurden, aus welchen Gründen sie die digitale Transformation in ihren Organisationen forcieren, nannten die Umfrageteilnehmer diese drei Faktoren mit Abstand am häufigsten: Kostensenkung, Förderung technischer Innovationen und Management von Cyberrisiken.

DIE WICHTIGSTEN GRÜNDE, AUS DENEN IT-VERANTWORTLICHE DIE DIGITALE TRANSFORMATION VORANTREIBEN, SIND:

- Reduzierung **der Kosten für** IT-Infrastruktur
- Förderung von Innovationen wie **5G und Edgecomputing**
- Minderung **des** Cybersicherheitsrisikos
- Management von **Multicloud-Umgebungen**
- Effektivere Rekrutierung von Spitzenkräften und **deren Bindung**

DIE WICHTIGSTEN GRÜNDE ZUR FORCIERUNG DER DIGITALEN TRANSFORMATION (NACH LAND)

Bewegen Sie den Mauszeiger auf die einzelnen Länder, um mehr zu erfahren.

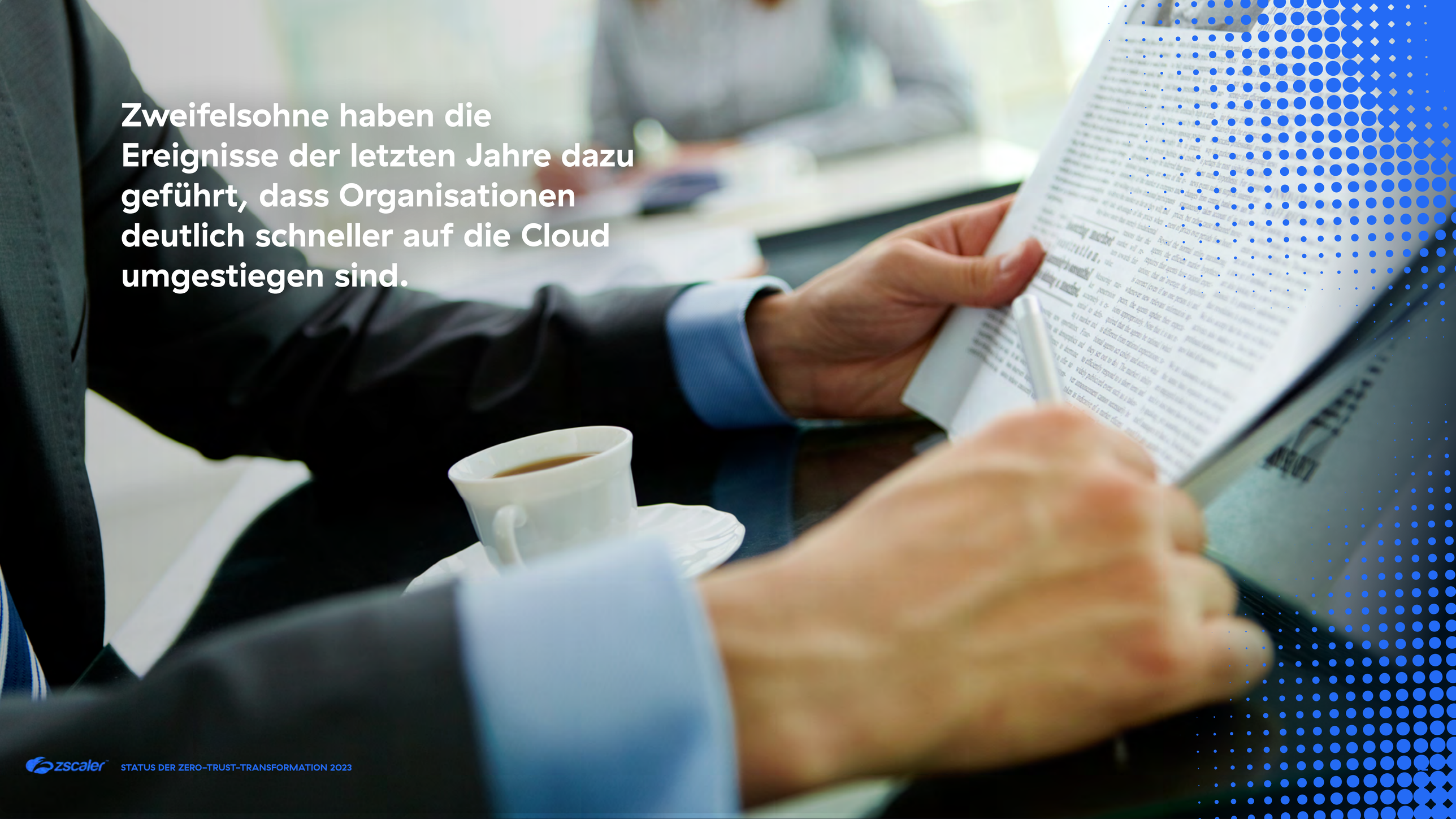
Die Ergebnisse aus Brasilien decken sich mit dem weltweiten Konsens: Die meisten Organisationen nannten die Reduzierung der IT-Infrastrukturkosten als Hauptgrund.

In einigen europäischen Ländern ergibt sich jedoch ein etwas anderes Bild. In Frankreich waren Organisationen am meisten daran interessiert, hybride Arbeitsmodelle umzusetzen, während in Schweden die Anwendererfahrung oberste Priorität hatte.

In zukunftsorientierteren Ländern wie Japan, Mexiko und Singapur war die Förderung von Innovationen wie 5G und Edgecomputing relevanter. Zudem nannten die Umfrageteilnehmer aus Singapur das Umsatzwachstum als wichtigen Faktor.

Die Optimierung von Geschäftsprozessen schaffte es in Brasilien und Spanien ebenfalls in die Top 3.

All dies sind sehr praktische Gründe, die auch allesamt von der IT forciert werden. Tatsächlich ist die hohe Bedeutung, die der Kostensenkung beigemessen wird, aktuell zwar sehr verständlich, diese Tatsache deutet jedoch auch darauf hin, dass möglicherweise immer noch deutliche Wissenslücken hinsichtlich der Hauptvorteile der Cloud bestehen. Und das wiederum könnte sich auf die Herangehensweise an und die Nutzung der Technologien auswirken, die zur Unterstützung der Cloud-Infrastruktur eingeführt werden — **beispielsweise Zero Trust.**



Zweifelsohne haben die Ereignisse der letzten Jahre dazu geführt, dass Organisationen deutlich schneller auf die Cloud umgestiegen sind.

Abschnitt II

Zero Trust als Sicherheitsmodell

Zero Trust ist ein ganzheitlicher Ansatz zum Schutz von Organisationen im Zeitalter der Digitalisierung. Er beruht auf dem Prinzip der minimalen Zugriffsrechte sowie dem Grundsatz, dass kein User und keine Anwendung automatisch als vertrauenswürdig gelten darf. Zero Trust geht von der Annahme aus, dass alle User und Anwendungen potenzielle Bedrohungen darstellen. Entsprechend wird Vertrauen nur basierend auf der Useridentität und dem Kontext gewährt, wobei Richtlinien bei jedem Schritt als Gatekeeper dienen. In den Vereinigten Staaten definiert das National Institute of Standards and Technology (NIST) das einer Zero-Trust-Architektur zugrunde liegende Prinzip folgendermaßen: Ressourcen oder Userkonten darf niemals allein aufgrund ihres physischen Aufenthaltsorts oder des Netzwerkstandorts (lokale Netzwerke gegenüber dem Internet) oder aufgrund der Herkunft der Ressourcen (Unternehmen oder Privatpersonen) vertraut werden. Das entspricht dem Grundsatz „niemals vertrauen, immer überprüfen“.

Angesichts der Tatsache, dass Sicherheit, Zugriff und Komplexität ganz oben auf der Agenda der IT-Verantwortlichen stehen, ist es nicht verwunderlich, dass sich immer mehr Organisationen für Zero Trust interessieren, um diese Herausforderungen zu bewältigen. Aus den Antworten der Umfrageteilnehmer geht hervor, dass Organisationen bereits über ein solides Verständnis der Sicherheitsvorteile von Zero Trust gegenüber herkömmlichen Ansätzen verfügen.

Als wir sie nach herkömmlicher Netzwerk- und Sicherheitsinfrastruktur fragten, gaben 54 % der IT-Verantwortlichen an, dass sie ihre Organisationen mit VPNs oder Perimeter-Firewalls nicht effizient vor Cyberangriffen schützen können und keine Transparenz über Anwendungstraffic und Angriffe erhalten. Weitere 68 % räumten entweder ein, dass Zero Trust Network Access (ZTNA) beim sicheren Remotezugriff auf Anwendungen eindeutige Vorteile gegenüber herkömmlichen Firewalls und VPNs bietet oder dass eine sichere Cloud-Transformation mit einer herkömmlichen Netzwerksicherheitsinfrastruktur nicht zu realisieren ist.

Bewegen Sie den Mauszeiger auf die einzelnen Länder, um mehr zu erfahren.

Umfrageteilnehmer, die der Meinung sind, dass eine sichere Cloud-Transformation mit einer herkömmlichen Netzwerksicherheitsinfrastruktur nicht möglich ist oder dass Zero Trust Network Access (ZTNA) eindeutige Vorteile gegenüber herkömmlichen Firewalls und VPNs bietet, wenn sicherer Remotezugriff auf Anwendungen bereitgestellt werden soll:

- 85 % Indien
- 81 % USA
- 75 % Brasilien
- 75 % Singapur
- 73 % Schweden

Umfrageteilnehmer, die der Meinung sind, dass VPNs/Perimeter-Firewalls entweder nicht effektiv vor Cyberangriffen schützen oder kaum Transparenz über Anwendungstraffic und Angriffe bieten:

- 72 % Indien
- 65 % Singapur
- 64 % Japan
- 57 % Deutschland
- 56 % USA

Teilnehmer, die der Meinung sind, dass IT-Teams neben Sicherheitslösungen auch integrierte Tools benötigen, um Probleme mit der Anwendererfahrung effektiv zu analysieren und zu beheben:

- 70 % Indien
- 63 % Mexiko
- 62 % USA
- 56 % Singapur
- 51 % Spanien
- 50 % Japan

90 %

Mehr als 90 % der Umfrageteilnehmer, die mit dem Umstieg auf die Cloud begonnen haben, haben bereits eine Zero-Trust-Sicherheitsstrategie implementiert oder planen, eine solche innerhalb der nächsten zwölf Monate einzuführen.

Als besonders vielversprechend erweist sich die Tatsache, dass die befragten Organisationen ihr ausgeprägtes Verständnis von Zero Trust auch praktisch anwenden. Mehr als 90 % der Befragten, die mit dem Umstieg auf die Cloud begonnen haben, haben bereits eine Zero-Trust-Sicherheitsstrategie implementiert, oder planen, eine solche innerhalb der nächsten zwölf Monate einzuführen.

Klare Spitzenreiter bei der Implementierung einer Zero-Trust-Strategie sind Italien und Indien: 97 % der italienischen und 96 % der indischen Organisationen geben an, dass sie entweder bereits über eine Strategie verfügen oder gerade im Begriff sind, eine solche einzuführen.

Bewegen Sie den Mauszeiger auf die einzelnen Länder, um mehr zu erfahren.

Prozentsatz der Organisationen, die Zero-Trust-Sicherheit bereits eingeführt haben, sie momentan implementieren oder sich gerade im Planungsprozess befinden:

- 97 % Italien
- 96 % Indien
- 95 % Vereinigtes Königreich
- 95 % USA
- 94 % Japan
- 93 % Brasilien
- 93 % Singapur
- 92 % Deutschland
- 91 % Mexiko
- 90 % Niederlande
- 89 % Spanien
- 89 % Frankreich
- 88 % Australien
- 85 % Schweden

Zero Trust wird immer noch vorwiegend als isolierte IT-orientierte (Sicherheits-)Lösung betrachtet — aber Organisationen könnten mit diesem Konzept so viel mehr erreichen.

Wenn Organisationen ein Zero-Trust-Sicherheitssystem eingerichtet haben oder planen, ein solches zu implementieren, bedeutet das leider nicht, dass sie es wirklich in vollem Umfang nutzen und Zero Trust somit als Business Enabler zum Einsatz kommt.

Tatsächlich weisen unsere Ergebnisse darauf hin, dass Zero Trust immer noch vorwiegend als isolierte, IT-orientierte (Sicherheits-)Lösung betrachtet wird. Das bedeutet, dass unmittelbare Herausforderungen im Bereich der Sicherheit angegangen und taktische Vorteile erzielt werden — aber Organisationen könnten mit Zero Trust so viel mehr erreichen.

DIE WICHTIGSTEN GRÜNDE FÜR DIE IMPLEMENTIERUNG EINER ZERO-TRUST-ARCHITEKTUR

65 % Optimierte Erkennung von komplexen Bedrohungen oder Angriffen auf Webanwendungen und erhöhte Sicherheit für sensible Daten

44 % Sicherer Remotezugriff für Anbieter, Partner und Betriebstechnologie

27 % Verbesserte sichere Konnektivität für hybride Mitarbeiter

24 % Geringere Kosten und Komplexität als bei Legacy-Netzwerksicherheit

HAUPTGRUND FÜR DIE IMPLEMENTIERUNG EINER ZERO-TRUST-INFRASTRUKTUR IN DEN UNTERSUCHTEN LÄNDERN:

Bewegen Sie den Mauszeiger auf die einzelnen Länder, um mehr zu erfahren.

Optimierte Erkennung von komplexen Bedrohungen:

- 52 % Indien
- 42 % Singapur
- 41 % USA
- 39 % Italien
- 35 % Spanien
- 30 % Frankreich
- 26 % Vereinigtes Königreich

Verbesserte Erkennung von Angriffen auf Webanwendungen:

- 44 % Brasilien
- 35 % Mexiko

Gesteigerte Sicherheit zum Schutz sensibler Daten:

- 44 % Brasilien

Bereitstellung von sicherem Remotezugriff für Anbieter, Partner und Auftragnehmer:

- 33 % Australien
- 32 % Japan
- 24 % Niederlande

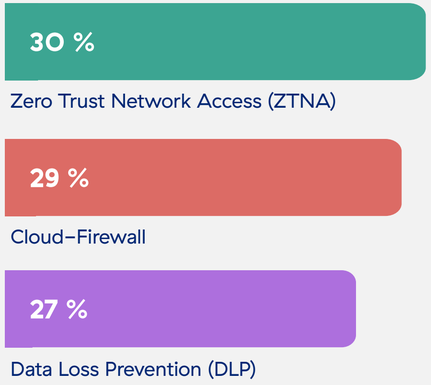
Dieser Zero-Trust-Ansatz — also ein Einsatz lediglich zu Beginn einer Transformation und ausschließlich aus Sicherheitsgründen — schränkt das Potenzial von Zero Trust erheblich ein — und das in einer Zeit, in der der Erfolg einer Organisation eng damit zusammenhängt, dass Digitalisierung und Innovationen schnell und in großem Maßstab vorangetrieben werden.

Wenn sich Organisationen des Konzepts hinter Zero Trust bewusst werden und es nicht nur als bloße Technologie oder Produkt betrachten, können sie ihre Infrastruktur vereinfachen, Geschäftsabläufe überdenken und letztlich die Transformation zu einer vollständig digitalisierten Organisation vollziehen. Organisationen, die das Zero-Trust-Prinzip umgesetzt haben, verfügen beispielsweise über ein lückenloses und genaues Inventar aller Anwendungen und aller in der Organisation vorhandenen Daten. Auf Grundlage dieser Bestandsaufnahme ist es dann möglich, strategische Entscheidungen darüber zu treffen, wie Prozesse optimiert, Kosten gesenkt, Legacy-Hardware abgeschafft und die Effizienz gesteigert werden soll.

Um aber diese strategischen Vorteile erschließen zu können, muss auch die Führungsebene umfassend informiert werden, sodass Zero Trust Teil der allgemeinen Organisationsstrategie wird. Momentan gibt es offensichtlich noch diverse Unsicherheiten und auch Kompetenzlücken in diesem Bereich, sodass vielen Entscheidungsträgern nicht vollumfänglich bewusst ist, was Zero Trust bedeutet und wie sich das Konzept auf ihre Organisation auswirken würde. Die aktuelle Herausforderung besteht darin, Führungskräften, einschließlich CIOs, zu vermitteln, dass das Ziel von Zero Trust darin besteht, die gesamte Infrastruktur zu vereinfachen, indem verwaltungsintensive Hardware entfernt wird. So erzielen Organisationen die gewünschten Geschäftsergebnisse und profitieren gleichzeitig von einem optimalen Sicherheitsstatus.

Ein Blick auf die Zero-Trust-Technologien, in die Organisationen in den nächsten zwölf Monaten vorrangig investieren wollen, zeigt, dass sich das Wissen um die geschäftlichen Vorteile weiterentwickelt — allerdings in den einzelnen Regionen in sehr unterschiedlichem Tempo und mit viel Raum für Verbesserungen.

DIE WICHTIGSTEN ZERO-TRUST-TECHNOLOGIEN, IN DIE ORGANISATIONEN INVESTIEREN



REGIONEN IM FOKUS: EIN EINDRUCK AUS NORD- UND SÜDAMERIKA

Amit Chaudhry, Senior Director, Product Marketing

Zur Steigerung der Agilität und Wettbewerbsfähigkeit setzen Organisationen heutzutage auf die Cloud, Mobilität, KI, IoT und Betriebstechnologie. User befinden sich überall, ebenso wie ihre Daten. Daher benötigen sie selbstverständlich jederzeit standortunabhängigen Direktzugriff auf Anwendungen, um schnell und produktiv zusammenzuarbeiten.

Das rasante Tempo des digitalen Wandels bietet Cyberkriminellen die Gelegenheit, jahrzehntealte Netzwerk- und Sicherheitsarchitekturen auszunutzen. Die Anzahl der Angriffe, insbesondere in Form von Ransomware und Angriffen auf die Lieferkette, ist mittlerweile auf einem absoluten Höchststand. Und da diese Angriffe immer raffinierter werden, reicht perimeterbasierte Sicherheit mit VPNs und Firewalls nicht mehr aus, um Netzwerke zu schützen und eine nahtlose Anwendererfahrung bereitzustellen.

Damit die Idee eines sicheren hybriden Arbeitsplatzes Wirklichkeit wird, wenden sich Organisationen von Firewalls und VPNs ab und führen stattdessen Zero-Trust-Architekturen ein, die jederzeit und überall schnellen Direktzugriff auf Anwendungen gewährleisten. Zero Trust basiert auf dem Prinzip der minimalen Zugriffsrechte, bei dem Verbindungen auf Grundlage von Identität und Kontext hergestellt werden. Damit ist Zero Trust vielleicht das einfachste, aber auch wirkungsvollste Konzept, um Daten effektiv zu schützen.

Momentan gibt es offensichtlich noch diverse Unsicherheiten und auch Kompetenzlücken in diesem Bereich, sodass nicht vollumfänglich klar ist, was Zero Trust bedeutet und wie sich das Konzept auf Organisationen auswirken könnte.

Abschnitt III

Umstieg auf Zero Trust zur Realisierung hybrider Arbeitsmodelle

Mit einer auf hybride Arbeitsmodelle ausgelegten Infrastruktur ist eine Infrastruktur gemeint, über die Mitarbeiter nahtlos zwischen physischen und Remote-Standorten hin- und herwechseln können, ohne dass es zu Einschränkungen und Verwaltungsaufwand kommt.

Als sich Organisationen durch die ersten Lockdowns gezwungen sahen, ihre Mitarbeiter im Homeoffice arbeiten zu lassen, ahnten wir nicht, dass diese „vorübergehende Maßnahme“ die Geburtsstunde eines völlig neuen Arbeitsmodells sein würde, das die gesamte Arbeitswelt in ihren Grundfesten erschüttert.

Die Arbeitnehmer von heute haben diverse Optionen: Sie können von zu Hause aus, im Büro oder an einem beliebigen anderen Standort arbeiten — und die Organisationen sollten über die dafür benötigten Technologien verfügen.

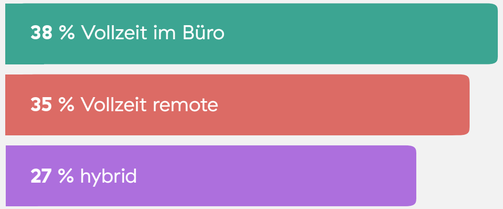
Die Umfrageteilnehmer gaben an, dass ihre Mitarbeiter auch in den nächsten 12 Monaten diese verschiedenen Möglichkeiten in vollem Umfang nutzen werden. Voraussichtlich werden 38 % Vollzeit im Büro, 35 % im Homeoffice und 27 % hybrid arbeiten. Diese Zahlen sind weltweit relativ einheitlich.

Fast zwei Drittel (62 %) der IT-Führungskräfte erklären, dass ihre Organisationen hybride Arbeitsmodelle oder die Arbeit im Homeoffice unterstützen. Die Prognose von mehr als einem Drittel (38 %), dass die Mitarbeiter wieder in Vollzeit im Büro arbeiten werden, ist jedoch sowohl überraschend als auch beunruhigend. In bestimmte Branchen, die auf persönliche Interaktionen angewiesen sind (z. B. Gesundheitswesen und Gastgewerbe), mag dies verständlich sein, doch bei günstigen Marktbedingungen könnte dieser Plan auch Probleme mit sich bringen. Beispielsweise besteht die Möglichkeit, dass Organisationen vor Schwierigkeiten bei der Rekrutierung von Fachkräften und der Mitarbeiterbindung stehen, wenn sie nicht in der Lage sind, die flexiblen Arbeitskonditionen zu bieten, die Mitarbeiter aufgrund ihrer Erfahrungen der letzten Jahre erwarten.

19 %

Weltweit gaben nur 19 % der befragten IT-Verantwortlichen an, dass bereits eine auf hybride Arbeit ausgerichtete Zero-Trust-Infrastruktur vorhanden ist.

PROZENTUALER ANTEIL DER BELEGSCHAFT, DER IN DEN NÄCHSTEN 12 MONATEN VORAUSSICHTLICH VOLLZEIT REMOTE, VOLLZEIT IM BÜRO ODER HYBRID ARBEITEN WIRD



Ob die IT- und Sicherheitsinfrastruktur überhaupt für diese Entwicklung gerüstet ist, ist jedoch eine ganz andere Frage. Weltweit gaben nur 19 % der befragten IT-Verantwortlichen an, dass bereits eine auf Hybridarbeit ausgerichtete Zero-Trust-Infrastruktur vorhanden ist. Das macht deutlich, dass die Organisationen noch nicht vollständig darauf vorbereitet sind, eine hochgradig verteilte Arbeitsumgebung umfassend zu unterstützen. Neben denjenigen, die ihre Infrastruktur bereits aktualisiert haben, sind weitere 50 % dabei, eine auf hybride Arbeit ausgerichtete Zero-Trust-Strategie zu implementieren, oder planen, eine solche Strategie einzuführen.

Diejenigen, die Zero Trust nutzen möchten, um Anbietern, Partnern, Auftragnehmern oder Fabrik- und Anlagenbetreibern — also Personenkreisen, die zwangsläufig in hybriden Umgebungen arbeiten — sicheren Remotezugriff bereitzustellen, geben an, innerhalb der nächsten zwölf Monate vorrangig in Zero Trust Network Access investieren zu wollen. Dies deutet darauf hin, dass der fortlaufenden Umstellung auf hybride Arbeitsmodelle unmittelbare Priorität eingeräumt wird.

Bewegen Sie den Mauszeiger auf die einzelnen Länder, um mehr zu erfahren.

Die Umsetzung einer auf hybride Arbeit ausgerichteten Zero-Trust-Strategie hat Priorität in:

- 37 % Indien
- 36 % Singapur
- 33 % Japan
- 29 % Deutschland
- 29 % Niederlande

Die folgenden Länder befinden sich überwiegend noch in der Planungsphase:

- 34 % Mexiko
- 27 % USA
- 27 % Frankreich
- 25 % Schweden

Insgesamt scheint das Vereinigte Königreich bei der Einführung von hybriden Zero-Trust-basierten Strategien am zögerlichsten zu sein: 21 % der Organisationen gaben an, dass sie derzeit nicht planen, eine hybride Infrastruktur einzuführen, und weitere 20 % ziehen es vor, bei ihren herkömmlichen Remotezugriffstechnologien zu bleiben.

Natürlich ist Sicherheit eine wesentliche Priorität für Organisationen, die zunehmend auf hybride Arbeitsmodelle umsteigen.

DIE WICHTIGSTEN HERAUSFORDERUNGEN BEZÜGLICH DER SICHERHEIT IN ORGANISATIONEN, DIE AUF HYBRIDE ARBEIT ÜBERGEHEN:

54 % sowohl Zugriff auf Betriebstechnologiesysteme als auch Internet

53 % Private On-Premise-Anwendungen oder private Anwendungen und Workloads in der Cloud (auf IaaS, PaaS)

32 % Internet der Dinge und Remotezugriff aufs Internet

Diese Ergebnisse zeigen aber auch, dass es bei der Sicherheit in einer hybriden Arbeitsumgebung nicht nur darum geht, Bedrohungen abzuwehren, sondern auch darum, für eine Vielzahl von Usern — von Mitarbeitern bis hin zu Lieferanten und Geschäftspartnern — sicheren Zugriff auf die Infrastruktur bereitzustellen.

Die Schwerpunktsetzung auf das Thema Sicherheit ist verständlich. Die genannten Gründe der Organisationen, die eine auf hybride Arbeitsmodelle ausgelegte Zero-Trust-basierte Infrastruktur implementieren oder einführen möchten, deuten aber auch auf die geschäftlichen Konsequenzen von Zero-Trust-Lösungen hin, die sich auf die Anwendererfahrung und Produktivität der Mitarbeiter auswirken.

GRÜNDE FÜR DIE IMPLEMENTIERUNG EINER AUF HYBRIDE ARBEITSMODELLE AUSGELEGTEN ZERO-TRUST-BASIERTEN INFRASTRUKTUR:

52 % Inkonsistente Anwendererfahrungen beim Zugriff auf On-Premise- und cloudbasierte Anwendungen und Daten

46 % Geringere Mitarbeiterproduktivität aufgrund von Problemen beim Netzwerkzugriff

39 % Fehlende Möglichkeiten, über persönliche Geräte auf Anwendungen und Daten zuzugreifen

Bewegen Sie den Mauszeiger auf die einzelnen Länder, um mehr zu erfahren.

Länder, die vergleichsweise häufig inkonsistente Anwendererfahrungen beim Zugriff angaben

- 70 % Japan
- 68 % Indien
- 64 % USA
- 62 % Singapur

In Europa gaben nur etwa die Hälfte der befragten Organisationen an, dass sie von solchen Problemen betroffen sind:

- 52 % Schweden
- 49 % Niederlande
- 47 % Frankreich
- 45 % Deutschland

Produktivitätsverluste aufgrund von Problemen beim Netzwerkzugriff wurden in folgenden Ländern als Hauptgrund für den Umstieg auf eine neue Infrastruktur genannt:

- 55 % Mexiko
- 48 % Spanien
- 47 % Vereinigtes Königreich

Die Befragten, deren Organisationen eine herkömmliche, VPN-basierte Infrastruktur für hybride Arbeit einsetzen, berichteten, dass sie sich immer noch mit einigen grundlegenden Herausforderungen der Remote-Arbeit auseinandersetzen müssen.

Die Anwendererfahrung ist entscheidend, um Produktivität in hybriden Arbeitsumgebungen zu gewährleisten — das ist eine der wichtigsten Erkenntnisse des letzten Jahres. Allerdings deuten unsere Ergebnisse darauf hin, dass die einzelnen Regionen ihre Infrastruktur unterschiedlich schnell modernisiert haben, um Probleme mit der Anwendererfahrung zu beheben.

Um in den heutigen, zunehmend verteilten Organisationsumgebungen eine optimale User Experience zu erzielen, sollten Organisationen den User-Traffic über den kürzesten Weg zur Anwendung leiten, damit Latenzen und Engpässe vermieden werden. Dabei müssen Organisationen berücksichtigen, dass moderne, hybride Mitarbeiter ausnehmend mobil sind: Von jedem Standort aus müssen User mit optimierter Bandbreite dynamisch zur gewünschten Anwendung weitergeleitet werden, egal, ob sie zu Hause, im Büro oder unterwegs arbeiten. Und sollte die Performance beim Zugriff auf geschäftskritische Anwendungen zu wünschen übrig lassen, kann es durchaus vorkommen, dass Mitarbeiter die Sicherheitskontrollen umgehen — ein nicht zu unterschätzendes Risiko.

Die Befragten, deren Organisationen eine herkömmliche, VPN-basierte Infrastruktur für hybride Arbeit einsetzen, berichteten, dass sie sich immer noch mit einigen grundlegenden Herausforderungen der Remote-Arbeit auseinandersetzen müssen. Dazu gehören die komplexe Verwaltung unterschiedlicher Sicherheitsinfrastrukturen für Mitarbeiter vor Ort und Remote-Mitarbeiter (47 %), langsame Anwendungsperformance (39 %) und Schwierigkeiten bei der Überwachung und Fehlerbehebung der Anwendererfahrung von Remote-Usern (37 %).

Zwar gibt es nach wie vor viele Sicherheitsbedenken im Zusammenhang mit der Umstellung auf hybride Arbeitsmodelle, doch spiegeln diese Antworten die viel umfangreicheren Herausforderungen wider, die hybrides Arbeiten für Organisationen darstellt — vor allem in den Bereichen Zugriff, Anwendererfahrung und Performance.

Wenn das Konzept richtig umgesetzt wird, bietet Zero Trust eine Lösung für all diese Probleme, sodass sich die IT umfassend auf die sich ständig ändernden Erwartungen und Geschäftsanforderungen konzentrieren kann.

REGIONEN IM FOKUS: EIN EINDRUCK AUS ASIEN–PAZIFIK

Heng Mok, CISO, APJ

Die Region Asien–Pazifik (APAC) ist ein hervorragendes Beispiel dafür, dass man nicht alles über einen Kamm scheren kann. Hier treffen die unterschiedlichsten Kulturen und Lebensstile aufeinander. Infolgedessen hat auch jeder Markt seine eigene Arbeitsweise — und das auch schon vor der Pandemie. Märkte wie Japan und Singapur sind geprägt von einer eher hierarchischen Struktur, wohingegen Australien und Indien traditionell lockerere Arbeitskonzepte verfolgen.

Da über einige Städte in der APAC–Region die härtesten Lockdowns der Welt verhängt wurden, sind diese Unterschiede jetzt, nachdem der Höhepunkt der Pandemie überstanden ist, noch deutlicher zu erkennen. Laut unserer Umfrage erwartet die Mehrheit der IT–Verantwortlichen aus Japan und Singapur, dass ihre Mitarbeiter zukünftig wieder Vollzeit im Büro arbeiten werden. Im absoluten Gegensatz dazu gehen die Befragten in Australien und Indien davon aus, dass ihre Belegschaft in Zukunft vollständig remote tätig sein wird.

Langfristig erwarten wir jedoch, dass noch mehr Organisationen auf hybride Arbeitsmodelle setzen werden. Viele Organisationen, mit denen wir gesprochen haben, entscheiden sich für hybride Arbeitsformen, um Vorteile bei der Rekrutierung von Spitzenkräften und der Mitarbeiterbindung zu erschließen. Angesichts des verschärften Wettbewerbs um einen begrenzten Mitarbeiterpool ist es nicht überraschend, dass viele Organisationen ähnliche Richtlinien einführen und nach Technologien suchen, die diesen Übergang nahtlos unterstützen.

Die Anwendererfahrung ist entscheidend, um Produktivität in hybriden Arbeitsumgebungen zu gewährleisten — das ist eine der wichtigsten Erkenntnisse des letzten Jahres.

Abschnitt IV

Ein Zero-Trust-Ansatz zur Integration aufstrebender Technologien

Der Begriff „aufstrebende Technologien“ bezieht sich auf neue oder sich schnell entwickelnde Technologien, deren praktische Anwendung noch weitgehend unerprobt ist, von denen aber erwartet wird, dass sie erhebliche Auswirkungen auf Organisationen haben und signifikante Wettbewerbsvorteile mit sich bringen.

Natürlich sind digitale Lösungen für die Remote-Arbeit nicht die einzigen Technologien, die Organisationen einsetzen möchten. Im heutigen Zeitalter der Digitalisierung spielt Betriebstechnologie eine immer größere Rolle. Als wesentlicher Bestandteil der kritischen Infrastruktur verließ sich dieses Segment in der Vergangenheit größtenteils auf Legacy-Systemen und veralteten Prozessen. Wir werden aber einen grundlegenden Wandel hin zu neuen, aufstrebenden Technologien erleben, die jeweils eigene vielversprechende Möglichkeiten zur weiteren Vereinfachung und Automatisierung von Geschäftsprozessen bieten.

Organisationen müssen jedoch noch vorausschauender handeln und auch weitere bevorstehende technologische Fortschritte berücksichtigen, um fundierte Entscheidungen über die Infrastruktur der Zukunft zu treffen. IT-Verantwortliche müssen sich mit allen Möglichkeiten vertraut machen, wie sich ihre Organisation durch Innovationen weiterentwickeln kann, und sich damit auseinandersetzen, wie sie ihre Geschäftsabläufe mithilfe von aufstrebenden Technologien effektiv unterstützen können. Mit Zero Trust haben Organisationen die Chance, sich schon heute auf innovative Technologien vorzubereiten und auf den Erfolg der Zukunft hinzuarbeiten.

In Übereinstimmung mit den untersuchten Beweggründen für die Cloud-Migration und die digitale Transformation im Allgemeinen haben unsere Ergebnisse verdeutlicht, dass bei der Planung neuer Technologieprojekte scheinbar keine umfassenderen strategischen Ziele verfolgt werden.

Auf die Frage nach der größten Herausforderung bei der Implementierung aufstrebender Technologien nannten 30 % der Befragten geeignete Sicherheitsmaßnahmen, gefolgt von den Budgetanforderungen für die weitere Digitalisierung (23 %). Allerdings gaben nur 19 % strategische Geschäftsentscheidungen als Herausforderung an.

DIE GRÖSSTE HERAUSFORDERUNG BEI DER IMPLEMENTIERUNG AUFSTREBENDER TECHNOLOGIEN (NACH REGION)

Bewegen Sie den Mauszeiger auf die einzelnen Länder, um mehr zu erfahren.

Sicherheit wurde in folgenden Ländern als größte Herausforderung wahrgenommen:

- 54 % Brasilien
- 41 % Japan
- 37 % Indien
- 37 % Italien
- 35 % Spanien
- 31 % USA

Unterdessen haben die folgenden Länder vor allem Schwierigkeiten mit den Budgetanforderungen:

- 27 % Singapur
- 27 % Frankreich
- 23 % Vereinigtes Königreich

Die Einführung aufstrebender Technologien scheint vor allem daran zu scheitern, dass Organisationen die entsprechende Zukunftsstrategie zu fehlen scheint.

- 24 % Niederlande

Das einzige Land, in dem die meisten Organisationen die Abhängigkeit von strategischen Geschäftsentscheidungen als größtes Hindernis nannten

- 28 % Schweden

Während die Sorgen um das Budget zu erwarten waren, ist der auf die Absicherung des Netzwerks gelegte Fokus interessant, bei dem gleichzeitig die strategische Geschäftsausrichtung vernachlässigt wird. Die Organisationen konzentrieren sich auf die Sicherheit, ohne sich des geschäftlichen Nutzens dieser Sicherheit bewusst zu sein — ein weiterer Beweis dafür, dass Zero Trust noch nicht als Business Enabler betrachtet wird.

Bei der Planung neuer Anwendungsfälle für aufstrebende Technologien wie Augmented Reality, digitale Zwillinge und virtuelle Konstruktionen sind niedrige Latenz und leistungsstarker Anwendungszugriff ebenfalls von Bedeutung. Dies gilt insbesondere für Nord- und Südamerika, wo das enorme Interesse an neuen Technologien auch in den nächsten drei Jahren nicht nachlassen wird.

RELEVANZ VON NIEDRIGER LATENZ UND LEISTUNGSSTARKEM ANWENDUNGSZUGRIFF IN DEN NÄCHSTEN DREI JAHREN

TECHNOLOGIEN MIT HÖCHSTER PRIORITÄT BIS 2025	WELTWEIT	EUROPA	NORD- UND SÜDAMERIKA	APAC
Cloudbasierter Zugriff auf Betriebstechnologie und industrielle Kontrollsysteme	34 %	29 %	40 %	38 %
Implementierung von 5G-Technologie für verbesserte Konnektivität	32 %	29 %	39 %	32 %
Reduzierung des CO2-Fußabdrucks	29 %	28 %	28 %	30 %
Umsetzung von Projekten im Bereich künstliche Intelligenz/maschinelles Lernen	27 %	22 %	39 %	28 %

Bewegen Sie den Mauszeiger auf die einzelnen Länder, um mehr zu erfahren.

Organisationen, die ihren Fokus auf cloudbasierten Zugriff für Betriebstechnologie und industrielle Kontrollsysteme legen:

- 46 % Mexiko
- 45 % Indien
- 44 % Singapur
- 36 % Australien
- 33 % Frankreich

Organisationen, die der Implementierung von 5G-Technologien oberste Priorität einräumen:

- 47 % Brasilien
- 45 % Indien
- 41 % Italien
- 36 % Spanien
- 28 % Vereinigtes Königreich

Organisationen, die die Reduzierung ihres CO2-Fußabdrucks priorisieren:

- 41 % Italien
- 28 % Deutschland
- 32 % Schweden

Nur Organisationen in den Niederlanden sehen die Ausweitung des Edgecomputing als besonders wichtig an (29 %), während sich die USA auf die Umsetzung von KI- und ML-Projekten konzentrieren (43 %).

Es ist bereits ersichtlich, dass diese priorisierten aufstrebenden Technologien zu weitreichenderen Geschäftskonsequenzen führen könnten. Die Umfrageergebnisse deuten jedoch darauf hin, dass es den meisten Organisationen an einer umfassenderen Zukunftsstrategie mangelt. Es bedarf einer viel bewussteren Ausrichtung auf die Wettbewerbsvorteile, die durch aufstrebende Technologien und deren strategischen Einsatz erzielt werden können — dazu gehört selbstverständlich auch deren effektive Absicherung.

REGIONEN IM FOKUS: EIN EINDRUCK AUS EMEA

Nathan Howe, VP of Emerging Technology

Europäische Organisationen sind in Bezug auf die Einführung neuer oder aufkommender Technologien eher selten die Vorreiter. Auch wenn Europa mit seinen mechanischen Erfindungen die Wiege der industriellen Revolution war, wurde die Region hinsichtlich der Einführung digitaler Technologien schon vor langer Zeit überholt. Stattdessen ist die APJ-Region zum Dreh- und Angelpunkt der Technologie rund um die Chipherstellung geworden, und innovationsfreudige Menschen aus aller Welt kommen in Silicon Valley zusammen, um transformative Technologien zu entwickeln.

Vor diesem Hintergrund ist es nicht verwunderlich, dass Asien das Potenzial von 5G als neue Form der Konnektivität, die weit über drahtlose Netzwerke hinausgeht, und als Grundlage für die Digitalisierung bereits erkannt hat. Während Nord- und Südamerika ähnliche Initiativen bereits gestartet hat, sind sich europäische Organisationen noch unsicher, wie sie ihre digitale Transformation mithilfe von 5G fördern können. Europa ist jedoch bereit, seinen Beitrag zur Cloud und aufstrebenden Technologien drastisch auszubauen, da sich die Länder durch aktuelle geopolitische Trends wie Lieferengpässe bei Chips und generelle Lieferkettenprobleme dazu gezwungen sehen, eigene Kompetenzzentren in der Region aufzubauen.

Abschnitt V

Der Schlüssel zur Erschließung des vollen Potenzials von Zero Trust

Wie können Organisationen diese Ergebnisse nun nutzen und ihre Zero-Trust-Einführung optimieren?

Die gravierenden Herausforderungen, die mit herkömmlichen Netzwerk- und Sicherheitsarchitekturen einhergehen, lassen sich nur durch ein Umdenken bewältigen. Legacy-Ansätze zur Gewährleistung der Konnektivität müssen radikal in Frage gestellt und durch Zero-Trust-Architekturen ersetzt werden, die auf dem Prinzip der minimalen Rechtevergabe basieren: User und Anwendungen dürfen niemals automatisch, sondern immer erst nach der Verifizierung von Identität und Kontext sowie entsprechenden Richtlinienkontrollen als vertrauenswürdig eingestuft werden.

Bei diesem Ansatz wird sämtliche Netzwerkkommunikation als potenzielle Bedrohung behandelt. Entsprechend wird Kommunikation zwischen Usern und Workloads bzw. zwischen Workloads blockiert, bis sie anhand identitätsbasierter Richtlinien validiert werden kann. Auf diese Weise lassen sich unbefugte Zugriffe und laterale Bewegungen zuverlässig verhindern. Diese Validierung wird in jeder Netzwerkumgebung durchgeführt, wobei der Netzwerkstandort einer Entität keine Rolle mehr spielt und keine rigide Netzwerksegmentierung erforderlich ist.

Zero Trust wurde zunächst als neue Methode zum Schutz von Netzwerken eingesetzt und schließlich über die On-Premise-Netzwerke hinaus ausgeweitet, war aber immer noch in erster Linie auf die Absicherung des privaten Anwendungsverkehrs ausgerichtet. Zu lange wurde Traffic nur basierend auf dem zugrundeliegenden Netzwerk betrachtet. Inzwischen hat sich jedoch gezeigt, dass die Grundsätze des Zero-Trust-Konzepts für eine Vielzahl weiterer Anwendungsfälle gelten. Insbesondere betrifft dies den Schutz von SaaS-Anwendungen, von ein- und ausgehendem Traffic in öffentlichen Clouds sowie von Usern, die auf das öffentliche Internet zugreifen. Weiter ist zu beachten, dass der Traffic nicht nur von Usern, sondern auch von Workloads ausgehen kann. Zugriffsrichtlinien können transportunabhängig durchgesetzt werden, d. h. es spielt keine Rolle, über welchen Router bzw. welches Netzwerk (kabelgebunden oder kabellos, 4G oder 5G etc.) der Traffic fließt.

Zero-Trust-Prinzipien müssen auf den gesamten Traffic — unabhängig vom Ursprung und Zielort — angewandt werden. Es sollte inzwischen nicht mehr darüber nachgedacht werden, welche Entität mit dem Netzwerk verbunden wird. Stattdessen sollten sämtliche Entitäten basierend auf Unternehmensrichtlinien direkt über eine Zero-Trust-Architektur miteinander verbunden werden. Im Zeitalter der Cloud fungiert das Internet als neues Unternehmensnetzwerk. Deshalb muss der gesamte Traffic untersucht werden, damit die richtigen Entitäten direkt über Unternehmensrichtlinien verbunden werden.

Welche Maßnahmen können Organisationen angesichts der aktuellen makroökonomischen Gegebenheiten und der neuen technologischen Anforderungen schon heute ergreifen, um die benötigte Sicherheit, Agilität, Flexibilität und Effizienz zu erreichen?

Diesbezüglich gibt es drei grundlegende Empfehlungen:

1

Organisationen müssen das Bild, das sie sich von Zero Trust gemacht haben, gründlich überdenken. Ein Zero-Trust-Ansatz bedeutet nicht nur Sicherheit, er fungiert auch als Wegbereiter der sicheren digitalen Transformation und Katalysator für den unternehmerischen Erfolg.

Eine Zero-Trust-basierte Architektur bietet ein höheres Maß an Transparenz sowie Kontrolle und reduziert die Komplexität der modernen IT. So können sich Organisationen auf die Ergebnisse konzentrieren, die sie von der eingesetzten Technologie erwarten — von hoher Performance über eine optimierte Anwendererfahrung bis hin zu geringeren Kosten.

2

Es besteht weiterhin ein verstärkter Bedarf an Aufklärung, um Bedenken, Unsicherheit und Zweifel darüber zu zerstreuen, was Zero Trust konkret bedeutet und wie Organisationen dieses Konzept optimal für sich nutzen können.

CIOs und CISOs übernehmen hier eine wichtige Rolle: Sie müssen der Vorstandsetage das Zero-Trust-Konzept in all seinen Facetten näherbringen und auch deutlich machen, wie sich dieser Ansatz gewinnbringend in die Unternehmensstrategie integrieren lässt.

3

Aufstrebende Technologien müssen als Wettbewerbsvorteil betrachtet werden, durch den sich schon bald deutliche Vorteile realisieren lassen — und mit einer Zero-Trust-fähigen Infrastruktur legen Sie schon heute den Grundstein für diese Zukunft.

Die Entscheidung darüber, welche aufstrebenden Technologien implementiert werden, sollte sich an der allgemeinen Geschäftsstrategie und aktuellen sowie zukünftigen Anforderungen der Organisation orientieren, nicht aber von temporären Trends und Modeerscheinungen beeinflusst werden. Zero Trust ist genau dazu gedacht, die Konnektivitätsanforderungen aufstrebender Technologietrends sicher und leistungsstark zu unterstützen.

Sobald Organisationen ihre Einstellung gegenüber Zero Trust überdacht haben und das Konzept als Business Enabler verstehen, müssen sie sich eine Frage stellen: Wie lässt sich eine effiziente Zero-Trust-Architektur implementieren, mit der man die gewünschten Ergebnisse erreicht?

Die Zscaler Zero Trust Exchange baut auf einer Zero-Trust-Architektur als Kernkomponente auf. Das Zero-Trust-Prinzip ist in sämtlichen Elementen des SSE-Frameworks inbegriffen: Das gilt für den User-Zugriff auf beliebige interne oder externe Anwendungen ebenso wie für die Anbindung von IoT sowie Betriebstechnologie und für alle Workloads, die in Multicloud-Umgebungen oder im Internet selbst auf Ressourcen zugreifen. Dank der Zero-Trust-Prinzipien können Sie standortunabhängiges hybrides Arbeiten als Teil der Geschäftsstrategie etablieren, wodurch Mitarbeiter, Geschäftspartner und Kunden die Möglichkeit haben, genau dort tätig zu sein, wo sie am produktivsten sind. Das ist eine wesentliche Voraussetzung für Business Continuity, die Anwerbung von Mitarbeitern, die nicht vor Ort arbeiten können oder wollen, und die Bereitstellung zunehmend beliebter hybrider Arbeitsumgebungen.

Als Cloud-nativer Service bietet die Zscaler Zero Trust Exchange Mitarbeitern, Geschäftspartnern sowie Kunden sicheren, schnellen und direkten Zugriff auf externe und interne Anwendungen — unabhängig von Standort, Gerät oder Netzwerk.

Die Zscaler-Plattform beinhaltet auch die sieben wesentlichen Bestandteile einer Zero-Trust-Architektur, die sich in die folgenden drei Kategorien unterteilen lassen:

Verifizierung

Die Zero-Trust-Architektur beendet zunächst die Verbindung und überprüft folgende Punkte:

1. Wer wird verbunden?
2. In welchem Kontext wird der Zugriff angefordert?
3. Wohin geht die Verbindung?

Kontrolle

Danach hat die Zero-Trust-Architektur folgende Aufgaben:

4. Bewertung von Risiken
5. Verhindern von Sicherheitsverletzungen
6. Verhindern von Datenverlusten

Durchsetzung

Bevor schließlich eine Verbindung hergestellt wird, führt die Zero-Trust-Architektur folgende Schritte aus:

7. Durchsetzen von Richtlinien

Unter Berücksichtigung dieser Bestandteile ist es Cloud-first-Organisationen problemlos möglich, ihre digitale Transformation zu beschleunigen und sich effektiv auf zukünftige Anforderungen vorzubereiten.

Zscaler und die Zscaler Zero Trust Exchange

Mit der größten, benutzerfreundlichsten und ausgereiftesten Zero-Trust-Plattform ist Zscaler unumstrittener Branchenführer im Bereich Zero Trust.

Im Rahmen Ihrer Zero-Trust-Einführung können Sie sich auf unsere Cloud-native Plattform Zscaler Zero Trust Exchange voll und ganz verlassen. Im Gegensatz zu Legacy-Netzwerk- und Sicherheitsprodukten handelt es sich bei der Zero Trust Exchange um eine speziell entwickelte Cloud-Plattform. Die Sicherheit beginnt mit dem Beenden jeder Verbindung, was eine eingehende Prüfung der Inhalte und eine Überprüfung der Zugriffsrechte auf der Grundlage von Identität und Kontext ermöglicht.

Die Zero Trust Exchange wird in 150 Rechenzentren weltweit bereitgestellt. Dadurch lässt sich die Verfügbarkeit in der Nähe der User und in Colocation mit häufig genutzten Cloud-Anbietern und Anwendungen wie Microsoft 365 und AWS gewährleisten. Organisationen profitieren von der kürzesten Verbindung zwischen Usern und Anwendungen, umfassendem Schutz und einer hervorragenden Anwendererfahrung.

Mehr über unsere benutzerfreundliche Plattform erfahren Sie hier.

Die Zero Trust Exchange ist in 150 Rechenzentren weltweit verfügbar

Methodik

ATOMIK Research befragte 1.908 leitende Entscheidungsträger (CIOs/CISOs/CDOs/Heads of Network Architecture) in EMEA (Vereinigtes Königreich, Deutschland, Frankreich, Niederlande, Schweden, Italien, Spanien), AMS (USA, Mexiko, Brasilien) und APAC (Japan, Indien, Australien, Singapur). Die Studie wurde zwischen dem 31. Mai und dem 28. Juni 2022 durchgeführt. Die Stichprobe bestand zu 43 % aus Organisationen mit bis zu 4.999 Mitarbeitern, zu 32 % aus Organisationen mit 5.000 bis 9.999 Mitarbeitern und zu 25 % aus Organisationen mit 10.000 oder mehr Mitarbeitern.