E-Book

Schützen Sie Ihre hybride Belegschaft mit ZTNA

10 unverzichtbare Merkmale einer unternehmenstauglichen ZTNA-Lösung

E-Book

Inhalt

Einführung

Die Arbeitswelt ist im Wandel. Überkommene Modelle zur Optimierung der Produktivität verlieren zunehmend an Bedeutung. Der Trend zur Umstellung auf Hybrid- und Remote-Arbeit hält weiter an. Entsprechend verlagern immer mehr Organisationen geschäftskritische Anwendungen in die Cloud, um die damit einhergehende Flexibilität, Skalierbarkeit und Effizienz voll ausschöpfen zu können.

Mit der Transformation der IT-Ökosysteme entstehen jedoch auch neue Risiken und Herausforderungen für Sicherheitsexperten. Durch die Unterstützung von Hybrid- und Remote-Arbeit für eine hohe Anzahl von Usern in Kombination mit verstärkter Nutzung der Cloud sowie des Mobilzugriffs kann sich die Angriffsfläche der Organisation vergrößern. Diese Gefahr besteht insbesondere, wenn versucht wird, diese Änderungen mit veralteten Ansätzen und Legacy-Sicherheitslösungen wie VPNs und Firewalls zu bewältigen.

Neben der größeren Angriffsfläche entstehen dadurch Transparenzlücken, die die zügige Untersuchung und Behebung von Sicherheitsvorfällen erschweren.

Bewältigen lassen sich diese Risiken nur durch ein neues Modell zur Sicherung von IT- und OT-Umgebungen, das heutigen Anforderungen an Sicherheit und Konnektivität gewachsen ist. Zero Trust erfüllt diese Ansprüche und setzt sich daher weltweit branchenübergreifend immer mehr durch.

Immer mehr Organisationen setzen auf Zero Trust Network Access (ZTNA) zur Stärkung ihres Sicherheitsstatus bei der Umstellung auf hybride Arbeitskonzepte. ZTNA empfiehlt sich als präzises, gut definiertes Framework, das die Umsetzung einer optimalen Zero-Trust-Strategie unterstützt. Die Branchenanalysten von Gartner bescheinigen dem ZTNA-Markt ein rasantes Wachstum von über 60 % gegenüber dem Vorjahr.

Organisationen nennen den Ersatz von Legacy-VPNs als wichtigste Motivation für die Implementierung von ZTNA.

Was ist Zero Trust Network Access (ZTNA)?

ZTNA umfasst eine Reihe von Technologien und Funktionen, durch die Remote-User sicher auf interne bzw. private Unternehmensanwendungen zugreifen können.

ZTNA basiert auf einem adaptiven Modell, bei dem keine Verbindung automatisch als vertrauenswürdig eingestuft wird. Zugriff wird nur nach Erforderlichkeit mit minimaler Rechtevergabe auf Basis granularer Richtlinien gewährt.

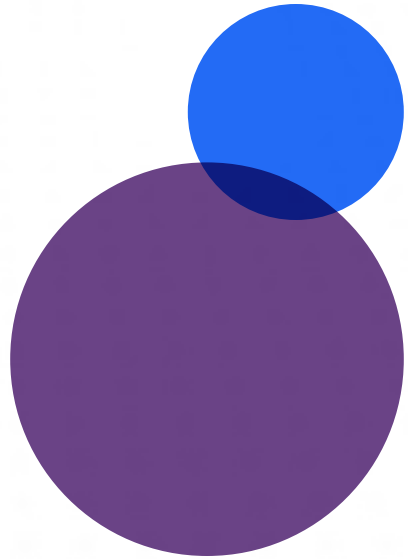
Im Zuge der Umstellung auf cloudbasierte Anwendungen und Infrastrukturen sind Organisationen zunehmend daran interessiert, ihre Sicherheitsservices mithilfe einer zentralen, ebenfalls in der Cloud bereitgestellten Plattform zu konsolidieren. Dies wird als Security Service Edge (SSE) bezeichnet. Neben ZTNA-Funktionen sind Secure Web Gateway (SWG) sowie Cloud Access Security Broker (CASB) im Leistungsumfang inbegriffen. Gartner empfiehlt den für Sicherheit und Risikomanagement zuständigen Entscheidungsträgern, die Umstellung auf ZTNA zum Ausgangspunkt für die Strategie zur Einführung von SSE zu machen. Insofern stellt sie oft einen entscheidenden ersten Schritt in Richtung cloudbasierter Sicherheit dar.

Viele Organisationen setzen auf ZTNA als Ersatz für VPN-Infrastrukturen, die sich schlecht skalieren lassen bzw. erhöhte Sicherheitsrisiken aufgrund der erweiterten Angriffsfläche verursachen. ZTNA ist jedoch viel mehr als eine effektivere Alternative zu VPN. Die Technologie bietet Organisationen die Möglichkeit, Legacy-Appliances (mitsamt dem dazugehörigen Verwaltungsaufwand) außer Betrieb zu nehmen und Usern schnellen Direktzugriff auf Anwendungen zu gewähren. Sie lässt sich mühelos skalieren und ermöglicht IT-Administratoren mehr Kontrolle und Transparenz.

Allerdings sind nicht alle auf dem Markt erhältlichen ZTNA-Produkte und -Lösungen gleichwertig. Organisationen, die von allen hier beschriebenen und weiteren Vorteilen profitieren wollen, sollten bei der Evaluierung geeigneter Lösungen darauf achten, ob sie die folgenden 10 Voraussetzungen erfüllen.

1. Eliminierung der Angriffsfläche, indem Anwendungen im öffentlichen Internet unsichtbar gemacht werden

In herkömmlichen Netzwerkarchitekturen, die auf dem Hub-and-Spoke-Modell basieren, haben Angreifer leichtes Spiel, sobald es ihnen gelingt, sich unbefugten Zugang zum Bereich innerhalb des Sicherheitsperimeters zu verschaffen.



Anwendungen und andere Ressourcen lassen sich durch eine einfache Suche problemlos aufspüren.

Eine echte ZTNA-Lösung vermittelt Direktverbindungen zu einzelnen Anwendungen. Selbst wenn es einem Angreifer gelingt, sich Zugriff auf eine Anwendung in Ihrer IT-Umgebung zu verschaffen, wird durch diese Segmentierung gewährleistet, dass alle übrigen Ressourcen innerhalb des Netzwerks für ihn unsichtbar bleiben.

Alle Anwendungen befinden sich hinter der ZTNA-Plattform und werden von ihr quasi abgeschirmt. Was Hacker nicht sehen können, ist vor Angriffen geschützt. Deswegen sollte eine ZTNA-Lösung IP-Adressen unkenntlich machen. Solche ausgehenden Verbindungen gewährleisten, dass sämtliche Anwendungen in Ihrem Ökosystem unsichtbar sind. Dadurch lassen sich gezielte Angriffe gegen einzelne Anwendungen verhindern.

2. Reibungslose Verbindungen unabhängig vom Standort

Bei 77 % aller Organisationen ist die Unterstützung von Hybridarbeit entweder bereits realisiert oder aktuell in Planung.

Legacy-Netzwerkarchitekturen basieren auf teuren MPLS-Verbindungen zwischen Zweigstellen und dem zentralen Rechenzentrum sowie auf Remotezugriff über VPNs. Je mehr sich Hybrid- und Remote-Arbeit als neue Normalität durchsetzen, desto mehr wird die VPN-Nutzung zum Problem. Das liegt vor allem daran, dass VPNs nicht skalierbar sind.

Im Gegensatz dazu trennt ZTNA den Zugriff auf Anwendungen vollständig vom Netzwerkzugang, sodass weder MPLS-Verbindungen noch VPNs erforderlich sind. Eine effektive ZTNA-Lösung sollte als cloudbasierter Service bereitgestellt werden, da dadurch die Notwendigkeit entfällt, den Traffic im Backhauling-Verfahren zum Rechenzentrum des Unternehmens umzuleiten. Stattdessen profitieren User von schnellem Direktzugriff auf die jeweils benötigte Anwendung.

Dabei sollten Sie auch bedenken, dass ein global aufgestellter ZTNA-Anbieter mit weltweit distribuierten Rechenzentren User und Anwendungen immer auf dem kürzesten Pfad verbinden kann. Durch die Vermittlung von Verbindungen möglichst nahe an der Edge wird standortunabhängig eine hervorragende User Experience für alle Mitarbeiter gewährleistet.

3. Zugriff mit minimaler Rechtevergabe

Minimale Rechtevergabe ist ein Grundprinzip des Zero-Trust-Konzepts. Es besagt ganz einfach, dass jedem User nur das Mindestniveau an Zugriffsberechtigungen zugewiesen wird, die für seinen jeweiligen Aufgabenbereich zwingend erforderlich sind.

Ohne die richtige ZTNA-Lösung kann der Aufbau einer entsprechenden Sicherheitsarchitektur schnell zur Herausforderung werden. Eine geeignete Lösung muss robuste Mechanismen zur Authentifizierung der User-Identität bereitstellen, Kontextdaten zu Geräten erfassen und analysieren und eine hochgradig granulare Segmentierung einzelner Verbindungen zwischen Usern und Anwendungen ermöglichen. Daher ist es wichtig, dass die ZTNA-Lösung umfassende Integrationen mit allen gängigen Identitätsanbietern unterstützt.

Am besten wählen Sie eine ZTNA-Lösung aus, die IT- und Geschäftsrichtlinien durchsetzen kann, indem verifizierte User nicht mit dem Netzwerk, sondern nur mit einzelnen Anwendungen gemäß ihren jeweiligen Berechtigungen verbunden werden. Zugriffsberechtigungen sollten unabhängig vom Standort — d. h. für Remote- und On-Premise-User — mit identischen Sicherheitskontrollen gewährt werden.

Zscaler unterstützte die Umstellung von 18.000 Mitarbeitern der Stadt Los Angeles auf sichere Remote-Arbeit.

Careem konnte die mittlere Reaktionszeit (MTTR) zur Behebung von Systemausfällen mit Zscaler Digital Experience Monitoring um 62 % verbessern.

4. Optimierung der Userproduktivität durch schnelle Erkennung und Behebung von Problemen mit Anwendungen, Netzwerken und Geräten [8]

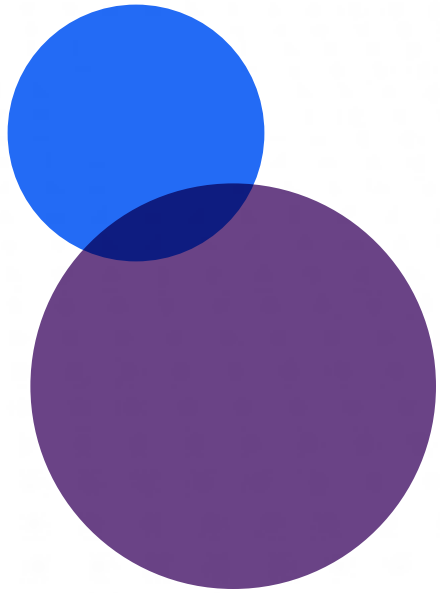
Die Umstellung auf Zero Trust setzt eine granulare Netzwerksegmentierung voraus — und zwar insbesondere bei Versuchen, sie mit Legacy-VPNs zu implementieren.

Dies ist schon rein technisch gesehen mit einigen Herausforderungen verbunden. Als erschwerender Faktor kommt die Notwendigkeit hinzu, eine optimale User Experience zu gewährleisten. Für Netzwerkbeauftragte und Servicedesk-Mitarbeiter ist es schwierig bis unmöglich, in segmentierten Netzwerken die erforderlichen Einblicke in die Performance von Enduser-Geräten und Anwendungen zu erhalten, um etwaige Probleme proaktiv zu erkennen und zu beheben.

Eine effektive ZTNA-Lösung sollte entsprechende Funktionen bereitstellen, die Ihre IT-Abteilung bei der Bewältigung dieser Schwierigkeiten unterstützen. Dazu zählt die Erfassung von Metriken zu Gerätezustand, Netzwerk-Performance und Verfügbarkeit von Anwendungen. Die Ergebnisse müssen auf einem übersichtlichen zentralen Dashboard angezeigt werden, damit Support-Mitarbeiter alle auftretenden Probleme frühzeitig erkennen und beheben können, bevor sie die User Experience beeinträchtigen.

5. Mikrosegmentierung auf Anwendungsebene zur Verhinderung lateraler Bewegungen

Eine ZTNA-Lösung sollte Ihre Daten, Workflows, Services und Ressourcen durch softwaredefinierte Mikrosegmentierung schützen. Das bedeutet, dass User direkt mit Anwendungen statt mit dem Netzwerk verbunden werden müssen.



Bei konsequenter Umsetzung gewährleistet dieser Ansatz, dass das Risiko lateraler Bewegungen im Netzwerk ausgeschaltet wird. Selbst wenn es Bedrohungsakteuren gelingt, einzelne User-Konten oder Anwendungen zu kompromittieren, haben sie keine Chance, den Angriff auf weitere Unternehmensressourcen auszuweiten.

Mit ZTNA werden User mit einzelnen Anwendungen bzw. Ressourcen verbunden, ohne automatischen Zugriff auf weitere Ressourcen zu erhalten.

Careem konnte die mittlere Reaktionszeit (MTTR) zur Behebung von Systemausfällen mit Zscaler Digital Experience Monitoring um 62 % verbessern.

6. Sicherer Zugriff für Privatgeräte der Mitarbeiter (BYOD) sowie unternehmenseigene Geräte

Eine geeignete ZTNA-Lösung sollte sowohl agentenbasierten als auch agentenlosen Zugriff für Mitarbeiter und externe Drittuser unterstützen.

Eine geeignete ZTNA-Lösung sollte sowohl agentenbasierten als auch agentenlosen Zugriff für Mitarbeiter und externe Drittuser unterstützen. Auf diese Weise kann ZTNA Geschäftspartnern und Dienstleistern nahtlosen Zugriff auf Ihre Ressourcen gewähren und gleichzeitig Mitarbeitern die sichere Nutzung von Privatgeräten (einschließlich Mobilgeräten) zur Erledigung ihrer Arbeit ermöglichen.

Zur Bewältigung der Risiken, die durch die Verwendung nicht verwalteter Geräte entstehen, muss eine ZTNA-Lösung außerdem über die Kapazitäten verfügen, um clientlosen Zugriff zu unterstützen. Andernfalls können Sie Ihre User nur schützen, wenn sie mit Geräten arbeiten, die vom Unternehmen bereitgestellt werden. Angesichts der zunehmenden Rolle von Mobilgeräten im Geschäftsalltag bedeutet das eine erhebliche Einschränkung.

7. Komplette Inline-Überprüfung des gesamten Traffics zur Abwehr von Angriffen und Blockierung von Bedrohungen

Die Blockierung sämtlicher Bedrohungen setzt lückenlose Transparenz voraus. Entsprechend muss eine ZTNA-Lösung in der Lage sein, eine komplette Inline-Überprüfung des gesamten Traffics durchzuführen.

Dies beinhaltet die Untersuchung des SSL-verschlüsselten Traffics, den Angreifer gerne zur unbemerkten Übertragung gefährlicher Inhalte wie Ransomware, Spyware oder Viren missbrauchen. Ausschließlich bekannte und als legitim eingestufte Kommunikationen dürfen zugelassen werden. Diese Inline-Überprüfung sollte auf Bedrohungsinformationen basieren, die aus einem breiten Spektrum globaler Signale gewonnen werden, um sicherzustellen, dass akute Ransomware-, Phishing- und Zero-Day-Bedrohungen sowie komplexe Angriffe zuverlässig blockiert werden.

Vor welchen Bedrohungen sollte eine effektive ZTNA-Lösung schützen? In den OWASP Top 10 werden die nach Expertenmeinung kritischsten Sicherheitsrisiken für Webanwendungen aufgeführt. Eine ZTNA-Lösung sollte zuverlässigen Schutz vor diesen und weiteren gängigen Angriffstechniken gewährleisten — insbesondere SQL-Injektion, Cross-Site-Scripting, Umgebungs- und Port-Scanner und Cookie-Poisoning.

Zscaler ermöglicht die Blockierung der OWASP Top 10 und anderer bekannter Sicherheitsrisiken für Webanwendungen, einschließlich SQL-Injection und Cross-Site-Scripting.

8. Nahtlose Integration mit einem breiten Spektrum von Identitätsanbietern und –lösungen

Zscaler verfügt über umfassende Integrationen mit Identitätsanbietern wie Microsoft und Okta sowie EDR–Plattformen (Endpoint Detection and Response) wie CrowdStrike.

Zero–Trust–Sicherheit beginnt mit der Verifizierung der Identität jedes Users, der versucht, Zugriff auf eine Anwendung oder eine andere Ressource zu erhalten.

Zur Unterstützung zukunftsfähiger Arbeitskonzepte setzen immer mehr Organisationen auf Cloud–first–Strategien und arbeiten dabei mit einem breiten Spektrum an IAM– (Identity and Access Management) bzw. IGA–Anbietern (Identity Governance and Administration) zusammen, um Authentifizierung und User–Identitäten langfristig effektiv verwalten zu können.

Eine ZTNA–Lösung sollte sich selbstverständlich mit Ihren aktuellen IAM– und IGA–Anbietern integrieren lassen. Zur Unterstützung Ihrer zukunftsfähigen Identitäts– und Authentifizierungsstrategie empfiehlt sich jedoch die Auswahl eines Anbieters, der zusätzlich über starke Geschäftsbeziehungen zu allen Branchenführern verfügt.

9. Integrierte Deception-Technologie zur Verhinderung von Angriffen

Als Deception-Technologie wird eine neue Kategorie von Cybersicherheitsmechanismen bezeichnet.

Sie ermöglicht die Früherkennung von Bedrohungen und zeichnet sich durch eine sehr geringe Fehlalarmquote aus. Der Ansatz beruht auf der Erstellung wirklichkeitsgetreuer Decoy-Ressourcen (z. B. Domains, Datenbanken, aktive Verzeichnisse, Server, Anwendungen, Dateien, Anmeldedaten und Breadcrumbs). Diese Decoys werden zusätzlich zu echten Ressourcen im Unternehmensnetzwerk platziert, wo sie quasi als Köder für potenzielle Angreifer fungieren. Sobald ein Angreifer sich unbefugten Zugang zum Netzwerk verschafft und mit den Decoys interagiert, werden Daten über seine Aktivitäten erfasst. Diese Informationen ermöglichen eine laufende Optimierung der Präzision und Zuverlässigkeit einschlägiger Warnmeldungen.

Durch Einsatz von Deception-Technologie optimieren Sie die Fähigkeit Ihres Sicherheitsteams zur Echtzeit-Erkennung von Bedrohungen und Risiken. Dadurch lassen sich Transparenzlücken in der IT-Umgebung effektiv schließen. Innerhalb einer Zero-Trust-Umgebung fungieren Deception-Decoys quasi als Stolperdrähte, deren Auslösung die Erkennung kompromittierter User-Konten bzw. unbefugter lateraler Bewegungen im Netzwerk ermöglicht.

Da es sich um eine sehr junge Technologie handelt, lassen integrierte Deception-Plattformen bei einigen ZTNA-Lösungen bislang auf sich warten. Bei den Branchenführern hat sich diese Neuerung hingegen bereits durchgesetzt.

KuppingerCole würdigt Zscaler als führenden Anbieter von Distributed-Deception-Plattformen.

10. Schnelle und unkomplizierte Bereitstellung

Im Gegensatz zu anderen Lösungen, deren Bereitstellung mehrere Wochen bis Monate in Anspruch nehmen kann, ist unsere branchenführende ZTNA-Technologie unabhängig von Ihrem Standort innerhalb weniger Tage einsatzbereit.

Mit Unterstützung von Zscaler konnte die Stadt Los Angeles in weniger als zwei Wochen sicheren standortunabhängigen Zugriff für 18.000 Mitarbeiter einrichten.

Zscaler Private Access: die weltweit am häufigsten eingesetzte ZTNA-Plattform

Zscaler Private Access (ZPA) erfüllt alle diese und weitere Anforderungen. ZPA basiert auf der marktführenden Zero-Trust-Architektur von Zscaler und unterstützt die konsequente Umsetzung einer minimalen Rechtevergabe. User erhalten dadurch sicheren Direktzugriff auf private Anwendungen, während gleichzeitig unbefugte Zugriffe und laterale Bewegungen verhindert werden. Als Cloud-nativer Service kann ZPA innerhalb weniger Stunden bereitgestellt werden, um Legacy-VPNs und Remotezugriffstools durch eine zukunftsfähige ganzheitliche Zero-Trust-Plattform zu ersetzen.

Zscaler Private Access bietet zahlreiche Vorteile:

- **Unübertroffene Sicherheit ohne Legacy-VPNs und Firewalls:** User werden nicht mit dem Netzwerk, sondern direkt mit der benötigten Anwendung verbunden. Dadurch wird die Angriffsfläche verkleinert und die laterale Ausbreitung von Bedrohungen verhindert.
- **Zuverlässiger Schutz für private Unternehmensanwendungen:** Durch branchenführenden Anwendungsschutz mit Inline-Funktionen zur Bedrohungsabwehr, Täuschungstechnologie und Bedrohungsisolierung lässt sich das Risiko kompromittierter User deutlich reduzieren.
- **Herausragende Produktivität für hybride Belegschaften:** Sekundenschneller Zugriff auf private Unternehmensanwendungen für Remote-User, Unternehmenszentrale, Zweigstellen und externe Geschäftspartner.
- **Einheitliche ZTNA-Plattform für User, Workloads und Geräte:** Der branchenweit einzigartige Funktionsumfang unserer ZTNA-Plattform gewährleistet sicheren Zugriff auf private Unternehmensanwendungen, Services, Betriebstechnologie und IoT-Geräte für Mitarbeiter und Geschäftspartner.

Sie möchten mehr erfahren? Fordern Sie noch heute eine kostenlose Produktdemo an.

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 SASE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Weitere Informationen finden Sie auf **zscaler.de** oder auf Twitter unter **@zscaler**.

+1 408 533 0288

Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA

zscaler.de