Sichere Remote-Verbindungen für heutige Geschäftsanforderungen

Inhaltsverzeichnis

Zusammenfassung

Viele Unternehmen verwenden virtuelle private Netzwerke (VPN), die den Datenverkehr wie durch einen Tunnel zurück zum Unternehmensnetzwerk übertragen. Sich jedoch bei der Sicherheit allein auf ein VPN zu verlassen, kann riskant sein. CISOs benötigen auch für die Zeit nach der Pandemie eine bessere Strategie zur Unterstützung von Homeoffices und Telearbeit, da wahrscheinlich viele Mitarbeiter zumindest zeitweise weiterhin außerhalb arbeiten werden. Angesichts der Grenzen von VPNs sowie der Dynamik und Dezentralität heutiger Netzwerke ist klar, dass eine bessere Lösung notwendig ist. Ein Zero Trust Network Access (ZTNA) ist die Weiterentwicklung des VPN-Fernzugriffs. Er vereinfacht die sichere Konnektivität und bietet nahtlosen Zugriff auf Anwendungen – unabhängig davon, wo sich Benutzer oder Applikationen befinden.

54 % der Mitarbeiter möchten auch nach der Corona-Pandemie die ganze oder meiste Zeit im Homeoffice arbeiten.[1]

Einleitung

Der jüngste Anstieg der Remote-Arbeit hat die Einschränkungen virtueller privater Netzwerke (VPNs) deutlich gemacht. VPNs sind seit Jahren der Standard für den Zugriff auf Unternehmensnetzwerke, haben jedoch einige große Nachteile, insbesondere bei der Sicherheit.

Das größte Problem ist der perimeterbasierte Sicherheitsansatz von VPNs: Benutzer stellen eine Verbindung über den VPN-Client her – und sind sie erst einmal im Unternehmensnetzwerk, können sie praktisch auf alles zugreifen. Das Netzwerk wird dadurch anfällig für Bedrohungen. Jedes Mal, wenn einem Gerät oder Benutzer auf diese Weise automatisch vertraut wird, sind die Daten, Anwendungen und das geistige Eigentum des Unternehmens gefährdet.

Netzwerk-Verantwortliche müssen nicht nur eine Lösung für dieses VPN-Problem finden, sondern auch Anwendungen besser schützen. Befinden sich einige Anwendungen in der Cloud und andere On-Premises, lässt sich oft nur schwer eine gemeinsame Sicherheitskontrolle und -durchsetzung realisieren. Zusätzlich erschwert wird dies, wenn nur ein Teil der Belegschaft im Unternehmen arbeitet, die andere Hälfte aber im Homeoffice oder von unterwegs aus. Werden dann Anwendungen in der Cloud bereitgestellt, steigt die Gefahr von Ausspäh-Angriffen – und das Risiko.

Stärkere Security als beim VPN

Ein Zero Trust Network Access (ZTNA) bietet eine bessere Lösung für Remote-Arbeit und den Anwendungszugriff. *Zero Trust* bedeutet „Null Vertrauen“: Bei diesem Sicherheitsmodell wird davon ausgegangen, dass kein Benutzer oder Gerät vertrauenswürdig ist. Auch wird für keine Transaktion ein Vertrauensvorschuss gewährt, ohne zuvor zu prüfen, ob der Benutzer und das Gerät zugriffsberechtigt sind.

Da der Zugang bei einem ZTNA-Modell grundsätzlich standortunabhängig ist, spielt es keine Rolle, ob ein Benutzer im Unternehmen oder außerhalb arbeitet. Es gilt immer der gleiche Zero-Trust-Ansatz – unabhängig davon, wo sich ein Benutzer oder ein Gerät physisch befindet. Wie der Name schon sagt, wird beim Zero-Trust-Ansatz davon ausgegangen, dass potenziell jedes Gerät infiziert ist und jeder Anwender zu böswilligem Verhalten fähig sein kann.

Anders als beim uneingeschränkten Zugriff über einen VPN-Tunnel gewährt das ZTNA-Modell den Zugriff pro Sitzung auf einzelne Anwendungen und Workflows erst, nachdem ein Benutzer und/oder ein Gerät überprüft und authentifiziert wurden. Dieser Zugang unterliegt enggefassten Richtlinien für den Anwendungszugriff. Die Autorisierung umfasst zudem zahlreiche Kontextinformationen, einschließlich Benutzerrolle, Gerätetyp, Gerätekonformität, Ort, Zeit und wie ein Gerät oder Anwender eine Verbindung zum Netzwerk oder zu einer Ressource herstellt.

Beim ZTNA-Modell wird der Zugriff erst erlaubt, wenn der Benutzer die richtigen Zugangsdaten (z. B. per Multi-Faktor-Authentifizierung) angegeben hat und das Endgerät (auch „Endpunkt“ genannt) überprüft wurde. Allerdings werden nur die absolut notwendigen Berechtigungen erteilt: Der Benutzer darf nur auf die Anwendungen zugreifen, die er zur effizienten Erledigung seiner Arbeit benötigt.

Die Zugangskontrolle endet nicht am Zugriffspunkt. Das ZTNA-Modell legt den Schwerpunkt auf die Identität, nicht auf einen „sicheren Ort im Netzwerk“. So lassen sich Anwendungen und andere Transaktionen von Ende zu Ende kontrollieren. Dank dieser umfassenderen Zugangskontrolle ist ein ZTNA nicht nur für Endanwender die effizientere Lösung, sondern sorgt auch für eine konsequentere Durchsetzung von Richtlinien.

Obwohl der ZTNA-Authentifizierungsprozess anders als bei einem herkömmlichen VPN mit Authentifizierungspunkten funktioniert, schreibt er nicht vor, wie die Authentifizierung erfolgen soll. Möchten Sie neue oder andere Authentifizierungslösungen implementieren, lassen sich diese problemlos zur ZTNA-Strategie hinzufügen. Neue Authentifizierungslösungen können z. B. dazu beitragen, Probleme durch schwache oder gestohlene Passwörter und Anmeldedaten zu beseitigen, unsichere IoT-Geräte (Internet der Dinge) besser zu schützen oder zusätzliche Verifizierungsstufen für den Zugriff auf sensible, vertrauliche Informationen oder kritische Ressourcen einzuführen.

ZTNA und VPN im Vergleich

Für Anwender ist ein ZTNA einfacher als ein VPN. Sie müssen sich weder den komplizierten VPN-Verbindungsaufbau noch die Anwendungen merken, für die der VPN-Zugang vorgeschrieben ist. Es besteht auch keine Gefahr durch offen gelassene Tunnel, weil jemand vergessen hat, die Verbindung zu trennen. Beim ZTNA klickt ein Benutzer einfach auf die Anwendung und erhält sofort eine sichere Verbindung – unabhängig davon, ob sich die Anwendung in einer Public oder Private Cloud oder On-Premises befindet. Dieser verschlüsselte Tunnel wird On-Demand erstellt und ist für Benutzer transparent. Er ist für interne und externe Anwender identisch, weil das Netzwerk keine grundsätzlich vertrauenswürdige Zone mehr ist. Die Security wird im Hintergrund bereitgestellt.

Es spielt wie gesagt keine Rolle, ob sich eine Anwendung in einer Private oder Public Cloud oder On-Premises befindet, da sich der Benutzer mit einem Durchsetzungspunkt verbindet und dann mit einer Proxy-Funktion auf die Anwendung zugreift. Die Anwendung muss lediglich eine Verbindung zu den Durchsetzungspunkten herstellen, um sie vor Ausspäh-Angriffen oder Bots zu schützen.

ZTNA-Modelle

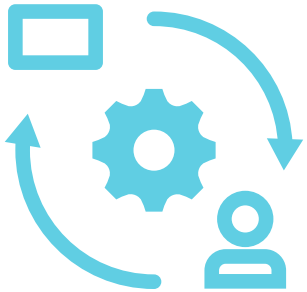
Auf dem Markt gibt es derzeit zwei Hauptkonzepte für die ZTNA-Implementierung: ein über Clients initiierter ZTNA und ein mit einem Dienst gestarteter ZTNA.

1. ZTNA mit Clients

Das ZTNA-Client-Modell – auch als „endpunktinitiierter ZTNA“ bezeichnet und ursprünglich als „softwaredefinierter Perimeter“ bekannt – basiert auf der Architektur der Cloud Security Alliance. Bei diesem Ansatz wird ein sicherer Tunnel mit einem Client aufgebaut, der auf dem Gerät installiert wurde. Möchte ein Benutzer auf eine Anwendung zugreifen, ermittelt der Client zuerst sein Sicherheits- bzw. Risikoprofil. Dafür werden Informationen über die Identität des Benutzers, den Gerätestandort, das Netzwerk und der verwendeten Anwendung erfasst. Anschließend wird über eine Proxy-Verbindung eine Verbindung zur Anwendung hergestellt. Entsprechen die Informationen den Unternehmensrichtlinien, wird der Zugriff auf die Anwendung gewährt. Dieses Verfahren gilt für alle Anwendungen: On-Premises und Software-as-a-Service (SaaS) in Clouds. Ohne ein zentrales Management für Implementierungen und Konfigurationen ist das Client-Modell jedoch schwer zu realisieren. Auch müssen nichtverwaltete Geräte anderes behandelt werden und erfordern u. U. einen Network Access Controller (NAC).

2. ZTNA mit Diensten

Das ZTNA-Dienstmodell verwendet eine Reverse-Proxy-Architektur (auch als „anwendungsinitiierter ZTNA“ bezeichnet). Es basiert auf dem BeyondCorp-Ansatz. Der größte Unterschied zum Client-ZTNA besteht darin, dass auf dem Endgerät kein Client installiert werden muss. Stattdessen baut ein Browser-Plugin den sicheren Tunnel auf, bewertet die Sicherheit des Geräts und erstellt das Risikoprofil. Ein großer Nachteil ist jedoch, dass dieses ZTNA-Modell nur für cloudbasierte Anwendungen funktioniert. Als Anwendungsprotokolle werden lediglich HTTP bzw. HTTPS akzeptiert, wodurch der ZTNA auf Webanwendungen und -protokolle wie Secure Shell (SSH) oder Remote Desktop Protocol (RDP) über HTTP beschränkt ist. Obwohl einige neuere Anbieter mehr Protokolle unterstützen, bleibt dieses ZTNA-Modell für alle Unternehmen ungeeignet, die eine Kombination aus Hybrid-Cloud- und On-Premises-Anwendungen nutzen.



„Gartner geht davon aus, dass sich 60 % der Unternehmen bis 2023 vom klassischen VPN verabschieden und auf ein ZTNA-Modell umstellen werden.“[2]

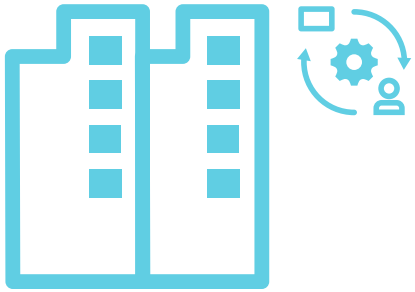
ZTNA und die Zukunft

Die Einführung eines Zero-Trust-Ansatzes für die Cyber-Sicherheit ist ein Prozess, der viele Systeme involviert und dessen unternehmensweite Umsetzung oft Jahre dauert. Dennoch ist eine bessere Regelung des Fernzugriffs ein sinnvoller erster Schritt zur Implementierung einer vollständigen Zero-Trust-Lösung.

Die meisten Unternehmen beginnen mit einer Mischung aus VPN und ZTNA. Viele ZTNA-Anbieter verwenden SASE-Dienste, die eine einfache Zugriffskontrolle auf Cloud-Anwendungen über die Cloud-Security ermöglichen. Solche Dienste können jedoch hohe SASE-Gebühren verursachen und unterstützen oft nicht alle Anwendungstypen.

Eine Zero-Trust-Komplettlösung für den Netzwerk-Zugriff erfordert mehrere Komponenten: einen Client, einen Proxy sowie eine Authentifizierung und Security. Häufig stammen diese Komponenten von mehreren Anbietern und verwenden unterschiedliche Betriebssysteme sowie verschiedene Management- und Konfigurations-Konsolen. Das Problem ist, dass sich mit Komponenten von unterschiedlichen Anbietern nur schwer ein lückenloses Zero-Trust-Konzept realisieren lässt.

Mit integrierten, automatisierten Tools lassen sich dagegen die wichtigsten Herausforderungen bei der ZTNA-Implementierung bewältigen. CISOs profitieren dabei besonders von einem integrierten SASE-Ansatz, der auf einer Firewall basiert. Dieser bietet einfach verwaltbare ZTNA-Funktionen, die für alle Benutzer – ob innerhalb oder außerhalb des Netzwerks – die gleichen anpassungsfähigen Anwendungszugriffsrichtlinien verwenden. Der ZTNA lässt sich für Remote-Anwender, Homeoffices und andere Standorte wie Einzelhandelsgeschäfte einsetzen. Unternehmen erhalten damit einen kontrollierten Fernzugriff auf Anwendungen, der einfacher und schneller zu starten ist und zugleich einen engmaschigeren Schutz als herkömmliche ältere VPNs bietet.



Nur 15 % der Unternehmen haben komplett auf ein Zero-Trust-Sicherheitsmodell umgestellt, das nicht automatisch davon ausgeht, dass jeder im Netzwerk vertrauenswürdig ist.[3]

Sicherer Fernzugriff mit ZTNA

Mit der Zunahme der Remote-Arbeit sind die Grenzen herkömmlicher VPNs deutlich geworden. Je mehr Menschen von überall arbeiten, desto unsicher wird der klassische perimeterbasierte Ansatz. Jedes Mal, wenn einem Gerät oder Benutzer automatisch vertraut wird, sind die Daten, Anwendungen und das geistige Eigentum des Unternehmens gefährdet. ZTNA-Lösungen bieten deshalb nicht nur einen stärkeren Schutz für den Remote Access, sondern verbessern auch die Kontrolle über den Anwendungszugriff.

[1] Kim Parker, et al.: „How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work". Pew Research Center, 9. Dezember 2020.

[2] Mike Wronski: „Since Remote Work Isn't Going Away, Security Should Be the Focus". Dark Reading, 24. September 2020.

[3] „2019 Zero Trust Adoption Report". Cybersecurity Insiders, November 2019.

FORTINET

www.fortinet.com/de

E-Book-ZTNA-Fernzugriff_DE

911928-0-0-DE