SOPHOS

Warum ZTNA so wichtig ist: Die Zukunft sicherer Netzwerke

ZTNA ermöglicht sicheren Remote-Zugriff und schützt vor Ransomware

Sophos-Whitepaper, 2022

Beim Thema Cybersecurity geht es im Wesentlichen um Risiko und Vertrauen. Vertrauen Sie dem Benutzer, der sich gerade am Netzwerk angemeldet hat? Oder dem, der versucht, auf Ihre Unternehmensanwendungen zuzugreifen? Und wie sieht es mit der E-Mail aus, die scheinbar von Ihrem Geschäftspartner stammt, jedoch ungewöhnliche Anfragen enthält? Handelt es sich dabei vielleicht um eine Betrugsmasche, eine so genannte Business Email Compromise? In den 1980ern lautete ein beliebtes Motto: „Vertrauen ist gut, Kontrolle ist besser". Mittlerweile gilt hingegen die Devise „Nichts und niemandem vertrauen, alles überprüfen".

So muss sich jeder beim Zero Trust-Modell vor dem Netzwerkzugriff authentifizieren. Doch das ist noch nicht alles. Bei jedem Versuch, auf eine Netzwerkressource zuzugreifen (z. B. einen Server, eine Anwendung oder Daten) werden die Geräte oder Anwendungen, über die der Zugriff erfolgt, zudem auf Compliance überprüft. Authentifizierung und Prüfung werden bei jeder neuen Anfrage wiederholt.

Aus Sicht der IT-Sicherheit gilt: Vertrauen ist nicht einfach da, es muss verdient werden. Bei jeder Benutzeranmeldung und jeder Aktion einer Anwendung oder eines Geräts im Netzwerk muss der Authentifizierungsprozess wiederholt werden.

Was ist ZTNA?

Zero Trust Network Access (ZTNA) basiert auf dem Zero-Trust-Prinzip: „Nichts und niemandem vertrauen, alles überprüfen". Dieser Ansatz bietet erheblich mehr Sicherheit: Alle Benutzer und Geräte bilden ihren eigenen Perimeter in ihrem eigenen Mikro-Segment des Netzwerks. Identität und Integrität werden beim Zugriff auf Unternehmensdaten und -anwendungen immer überprüft. Benutzer dürfen nur auf Anwendungen und Daten zugreifen, die explizit in den entsprechenden Richtlinien definiert sind. Dies minimiert laterale Bewegungen sowie damit verbundene Risiken.

Ransomware-Opfer sind in der Regel wesentlich mehr mit ZTNA vertraut. Aller Wahrscheinlichkeit nach ist dies auf das Bestreben zurückzuführen, erneute Angriffe zu verhindern. Im weiteren Verlauf gehen wir noch näher darauf ein, was unsere Kunden über ZTNA denken und wie sie die Technologie nutzen.

ZTNA ist ein wesentlicher Bestandteil eines SASE (Secure Access Service Edge)-Security-Frameworks, das Netzwerk- und Cloud-Security-Funktionen über eine zentrale Cloud-Plattform bereitstellt. Der Begriff „SASE" wurde 2019 vom Analystenhaus Gartner geprägt und beschreibt die Kombination von herkömmlichen WAN-Verwaltungs- und Security-Funktionen unter Verwendung cloudnativer Architekturen. Neben ZTNA umfasst die SASE-Architektur außerdem Cloud Access Security Broker, Firewall-as-a-Service, Intrusion-Prevention-Systeme sowie sichere Access Gateways.

Cloud-Management bietet zahlreiche Vorteile: sofortige Inbetriebnahme, reduzierte Management-Infrastruktur, schnelle Bereitstellung und Registrierung sowie standortunabhängigen Zugriff. So können sich Ihre Benutzer sofort anmelden und produktiv arbeiten, ohne dass Sie in zusätzliche Management-Server oder -Infrastruktur investieren müssen. Cloud-Management sorgt außerdem für sofortigen, sicheren Zugriff von überall, auf allen Geräten und unterstützt so Ihre gewünschte Arbeitsweise. Zudem lassen sich neue Benutzer schnell und einfach registrieren – ganz unabhängig davon, wo sie sich gerade befinden.

Ein Umstieg auf ZTNA bietet erheblich mehr Sicherheit für mobile Mitarbeiter und von der Pandemie geprägte Netzwerkumgebungen mit einer hohen Anzahl an Remote-Benutzern. Zudem schützt ZTNA Ihr Unternehmensnetzwerk vor Malware und Ransomware-Angriffen.

Warum VPN so problematisch ist

So schrecklich die Pandemie auf menschlicher Ebene auch war, so brachte sie doch eine unerwartete, aber bedeutende Innovation im Bereich Remote Access mit sich: ZTNA als Alternative für anfällige VPN-Clients. Im Zuge der Pandemie gingen Millionen von Mitarbeitern ihrer Tätigkeit im Homeoffice nach. Dabei entstanden Millionen neuer, anfälliger Endpoints, die häufig nicht von der Unternehmens-IT kontrolliert werden konnten.

Da ein beträchtlicher Anteil dieser Endpoints möglicherweise nicht über adäquaten Schutz verfügt, stellen sie ein attraktives Ziel für Angreifer dar. Zudem waren Unternehmens-VPNs nicht für den rapiden Anstieg an Remote-Benutzern ausgelegt und somit überlastet.

ZTNA basiert auf dem Zero-Trust-Prinzip. Gleichzeitig löst ZTNA den traditionellen Remote-Zugriff über VPN ab, eine Methode, die Benutzer vor viele Herausforderungen stellt. In technologischer Hinsicht weisen VPNs drei wesentliche Nachteile für zunehmend mobile Teams auf.

Zum einen sind VPNs nur bedingt skalierbar und werden den Anforderungen großer Unternehmen mit einem hohen Anteil an Remote-Benutzern nicht gerecht. Zum anderen ist VPN-Client-Software häufig veraltet, nicht hinreichend gewartet und komplex und stellt somit ein potenzielles Ziel für Angreifer dar. Häufig weisen VPNs zudem Schwachstellen auf, da sie sich in puncto Sicherheit auf traditionellen Zugriff mit Benutzernamen und Passwort beschränken. Außerdem besitzen Benutzer, die sich effektiv über VPNs mit dem Unternehmensnetzwerk verbinden, uneingeschränkten Zugriff. Vergleichbar ist dies etwa mit einem Arbeitsplatzrechner innerhalb der Perimeter-Firewall. Je nach den internen Netzwerkkontrollen kann dies problematisch sein.

Sehen wir uns jetzt die einzelnen Probleme genauer an und wie ZTNA diese lösen kann.

VPNs lassen sich nur bedingt skalieren. Die maximale Bandbreite von VPNs ist häufig auf 1 GBit/s beschränkt. Zudem bergen ungeschützte Ports und überprivilegierter Zugriff Sicherheitsrisiken. Auch sind VPNs anfällig für Man-in-the-Middle-Angriffe. Hinzu kommt, dass VPNs für eine bestimme Anzahl an Remote-Benutzern ausgelegt sind und sich nicht dynamisch herauf- oder herabskalieren lassen. So können Benutzer eventuell erst dann auf das VPN zugreifen, wenn andere ihre Verbindung trennen.

In den letzten Jahren hat die US-Behörde NSA auch immer wieder in Sicherheitshinweisen vor VPN-Sicherheitslücken gewarnt. 2019 veröffentlichte das kanadische Zentrum für Cybersicherheit einen Leitfaden, aus dem hervorging, dass drei beliebte VPN-Produkte mehrere Kompromittierungs-Indikatoren aufwiesen. Hierzu zählten Zurücksetzungen von Anmeldeinformationen sowie anfällige proprietäre SSL- und TLS-VPN-Protokolle.

Außerdem bieten VPNs keinerlei Filter für den Benutzerzugriff auf das Netzwerk. Benutzer besitzen im Grunde die gleichen Rechte wie ein Arbeitsplatzrechner hinter der Unternehmens-Firewall.

Das Risiko, dass Angreifer Remote-Access-Tools dazu missbrauchen, sich im Netzwerk zu bewegen, lässt sich anhand der beiden folgenden Methoden minimieren: Zum einen können Sie festlegen, dass sich jeder Benutzer, jedes Gerät und jede Anwendung vor dem Netzwerkzugriff authentifizieren muss. Dabei darf sich der Zugriff nur auf ein bestimmtes Mikrosegment des Netzwerks beschränken. So können sich erfolgreiche Angreifer nur begrenzt im Netzwerk bewegen. Zum anderen sollten Sie die Rechte aller Benutzer im Netzwerk auf das Nötigste beschränken. Wenn Angreifer das Netzwerk aufgrund eingeschränkter Rechte nicht sehen, können sie es auch nicht durchsuchen.

Im Report „The Forrester New Wave: Zero Trust Network Access, Q3 2021" heißt es dazu: „Mit ZTNA greifen Benutzer auf der Basis von Zero-Trust-Prinzipien auf lokale Anwendungen zu. Bidirektionaler Datenverkehr von Videokonferenzen läuft dabei direkt ins Internet. Dies sorgt für mehr Sicherheit und eine bessere User Experience. Letztendlich reduziert ZTNA den Bedarf an Mitarbeiter-VPNs. So können Infrastruktur- und Sicherheitsteams auf in der Cloud bereitgestellte Netzwerk- und Security-Funktionen umsteigen."

Sorglos-Sicherheit dank ZTNA

Im Sinne der Corporate Governance steht die Kontrolle darüber, wer im Netzwerk welche Aufgaben ausführt, an erster Stelle. Corporate Governance beinhaltet Richtlinien und Prozesse für Betriebsabläufe sowie ethische Geschäftspraktiken, die finanzielle Rentabilität möglich machen. Es kann vorkommen, dass Bedrohungsakteure ihr Unwesen im Netzwerk treiben, vertrauliche Daten kompromittieren oder stehlen, Ransomware oder sonstige Malware installieren oder ganz einfach unbemerkt auf einen günstigen Angriffszeitpunkt warten. Mögliche Konsequenzen sind nicht nur eine Verletzung von Compliance-Auflagen und ein erheblicher finanzieller Aufwand. Solche Angriffe können auch den Marktwert eines Unternehmens beträchtlich herabsetzen.

Mit Hilfe von Zero-Trust-Netzwerk-Modellen im Allgemeinen und ZTNA im Speziellen lassen sich Angreifer im Netzwerk und unbefugte Benutzer ermitteln sowie schädliche von vertrauenswürdigen Anwendungen unterscheiden. Dabei können Unternehmen ihre Angriffsfläche um ein Vielfaches reduzieren und das Risikoprofil des Unternehmens optimieren.

Wenn sich Benutzer über ZTNA am Unternehmensnetzwerk anmelden, greifen Geräte auf Ressourcen in ihrem eigenen mikro-segmentierten Perimeter zu, der ständig validiert und verifiziert wird. Bei Zero Trust befinden sich die Benutzer nicht mehr „im Unternehmensnetzwerk", in dem jedem implizit vertraut und Zugriff gewährt wird. Vielmehr können sie ausschließlich auf die Netzwerkbereiche zugreifen, für die sie und ihre Geräte authentifiziert wurden. Bei Legacy-VPN-Verbindungen ist dies nicht der Fall.

Bei herkömmlichen Netzwerken wehrt die Unternehmens-Firewall Angreifer ab. Wenn Anmeldeinformationen jedoch erst einmal akzeptiert wurden, können sich Angreifer frei bewegen. Erlangen sie dann erhöhte Benutzerrechte, können sie in abgesicherte Netzwerkbereiche vordringen, Daten stehlen, kopieren oder verschlüsseln, um Lösegeld zu erpressen.

Wenn Unternehmen auf eine Zero-Trust-Architektur umsteigen, sind gestohlene Zugangsdaten für Angreifer praktisch wertlos. Auch bildet die Firewall dann nur die erste Stufe von zahlreichen weiteren Schutzmechanismen für Dateien und Anwendungen. Auch wenn ein Computer eines Mitarbeiters im Homeoffice kompromittiert wird, können Angreifer mit den Zugangsdaten des Mitarbeiters nicht auf das gesamte Unternehmensnetzwerk zugreifen.

Bei ZTNA-Lösungen beschränkt sich der Netzwerkzugriff nämlich auf einen begrenzten Bereich. Und dazu müssen Angreifer erst einmal über die Anmeldeinformationen verfügen, um sich, das Gerät und die Software für eine vertrauenswürdige Anwendung oder Daten zu authentifizieren.

Keine Chance für Ransomware

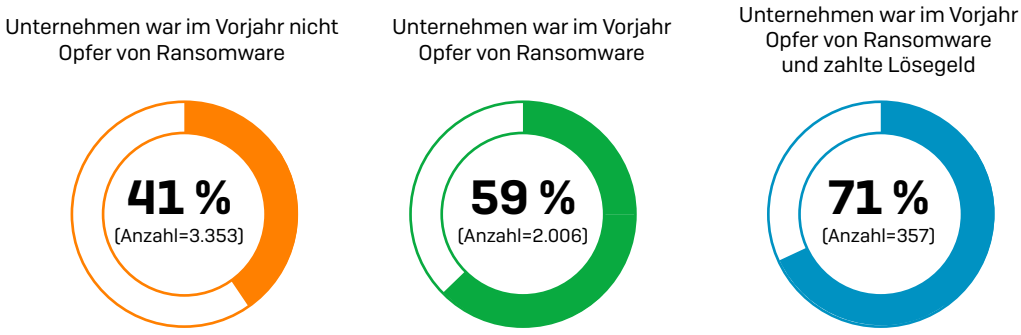
Im Rahmen einer von Sophos in Auftrag gegebenen und von Vanson Bourne durchgeführten Befragung von 5.400 IT-Experten aus aller Welt gaben 20 % der Umfrageteilnehmer an, dass sie Zero Trust bereits eingeführt haben. Weitere 41 % gehen davon aus, dass sie die Implementierung bis Anfang 2022 zum Abschluss bringen werden. 20 % der befragten Unternehmen planen die Implementierung von ZTNA bis Anfang 2023.

ZTNA-Lösungen beseitigen einen gängigen Angriffsvektor für Ransomware und andere Angriffsarten, die darauf abzielen, das Netzwerk zu infiltrieren. Da sich ZTNA-Benutzer nicht mehr „im Netzwerk", sondern in einem Mikro-Segment des Unternehmensnetzwerks befinden, haben Bedrohungen, die bei VPN im Netzwerk möglicherweise Fuß fassen, mit ZTNA keine Chance.

Ransomware-Angriffe treiben den Wechsel zu ZTNA voran

Wie unsere Umfrage zeigt, sind Unternehmen, die im Vorjahr von Ransomware betroffen waren, mit 50 % höherer Wahrscheinlichkeit bereits „sehr mit dem ZTNA-Prinzip vertraut" gegenüber Unternehmen, die von Ransomware-Angriffen verschont blieben (59 % ggü. 39 %). Bei Ransomware-Opfern, die das Lösegeld bezahlten, liegt der prozentuale Anteil bei ganzen 71 %.

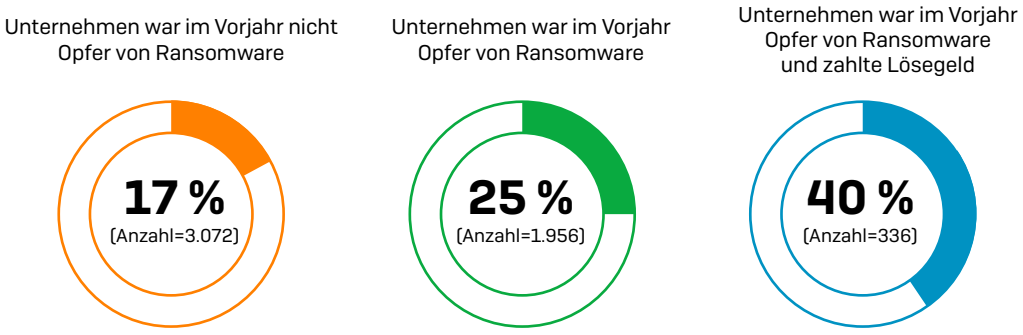
Prozentualer Anteil der befragten Unternehmen, die sich selbst als „sehr vertraut" mit Zero Trust Network Access einschätzen



Auch sind lediglich 10 % der von Ransomware betroffenen Unternehmen kaum oder gar nicht mit ZTNA vertraut. Bei Unternehmen, die keine Ransomware-Angriffe verzeichneten, sind es 21 %.

Darüber hinaus zeigte die Umfrage, dass die Implementierung von ZTNA bei Ransomware-Opfern weiter fortgeschritten ist. Ein Viertel (25 %) der Unternehmen, die im Vorjahr einen Ransomware-Angriff hinnehmen mussten, ist bereits vollständig auf Zero Trust umgestiegen. Bei betroffenen Unternehmen, die das Lösegeld zahlten, liegt der prozentuale Anteil bei ganzen 40 %. Zum Vergleich: Nur eines von sechs Unternehmen (17 %), die noch nicht von Ransomware betroffen waren, hat bereits vollständig auf ZTNA umgestellt.

Prozentualer Anteil der befragten Unternehmen, die bereits einen Zero-Trust-Ansatz verfolgen



Darüber hinaus haben Ransomware-Opfer unterschiedliche Beweggründe für die Einführung von ZTNA.

- Bei den Antworten auf die Frage, aus welchen Gründen sich Unternehmen für das Zero-Trust-Prinzip entscheiden, lassen sich durchaus Gemeinsamkeiten, jedoch auch klare Unterschiede erkennen. Die meisten Unternehmen verfolgten das Ziel, „ihren Sicherheitsstatus insgesamt zu verbessern" – und zwar unabhängig davon, ob sie von Ransomware betroffen waren oder nicht
- Als zweitwichtigsten Grund führten Ransomware-Opfer das Ziel an, „ihre Cybersecurity Operations zu vereinfachen" (43 %). Dies lässt sich vielleicht dadurch erklären, dass eine komplexe IT-Security den Ransomware-Angriff mitverschuldet hatte
- Zudem begründeten Ransomware-Opfer den Umstieg auf Zero Trust häufiger mit einem „Wechsel von einem CAPEX- zu einem OPEX-Modell" (27 % ggü. 16 %; bei Unternehmen, die von Ransomware betroffen waren und das Lösegeld zahlten, lag der prozentuale Anteil bei 34 %)
- Ein weiterer wichtiger Beweggrund von Ransomware-Opfern bestand darin, ihr Unternehmen „bei der zunehmenden Nutzung der Cloud zu unterstützen" (42 %). Von den Unternehmen, die in letzter Zeit keine Angriffe verzeichneten, wählten lediglich 30 % diese Antwort aus

Ein Ausblick

Es ist nicht immer einfach, die Geschäftsleitung und Aktionäre von den Vorteilen einer Zero-Trust-Umgebung zu überzeugen. Denn es lässt sich nur schwer belegen, dass Angriffe vereitelt wurden oder gar nicht stattgefunden haben, weil Cyberkriminelle ihre Malware nicht einschleusen konnten. Es lässt sich jedoch durchaus nachweisen, dass Zero Trust Risiken erheblich reduziert. Und das spart Unternehmen Geld.

So kann ein geringeres Unternehmensrisiko etwa mit niedrigeren Versicherungsprämien oder günstigeren Konditionen für eine Cyberversicherung einhergehen. Auch die Unternehmensbewertung steigt potenziell. Cyber-Versicherungsunternehmen erkennen an, dass ein geringeres Risiko zu weniger Schadenfällen führt und dementsprechend auch Auszahlungen zurückgehen. Vor diesem Hintergrund überarbeitet die Cyber-Versicherungsbranche derzeit ihre Vertragsbedingungen. So erhalten Unternehmen, die ihr Risiko proaktiv reduzieren, auch entsprechend bessere Konditionen.

Auch Gartner sieht in Zero Trust die Zukunft der Cybersecurity. „Sowohl für große Unternehmen, deren Cloud-Transformation bereits weit fortgeschritten ist, als für auch solche, die noch am Anfang stehen, muss der Schutz von Daten höchste Priorität einnehmen“, so Gartner. Den Marktforschern von Gartner zufolge möchten 82 % der Unternehmen ihren Mitarbeitern längerfristig eine Option auf Homeoffice anbieten. „Da Unternehmen mobile Arbeitsformen zunehmend in ihre langfristige Planung aufnehmen, spielt das Thema Sicherheit eine immer wichtigere Rolle. Dabei stellen viele Unternehmen jedoch fest, dass ihre bisherigen Sicherheitsstrategien nicht für cloudnative mobile Teams ausgelegt waren“, so Gartner.

Forrester stimmt dem zu und erklärt, dass Zero Trust Ressourcen und nicht das physische Netzwerk schützt. „In seiner einfachsten Form verlagert das Zero-Trust-Modell den Fokus von diversen Formen der Authentifizierung hin zu benutzerdefinierten Datenspeichern, Anwendungen, Systemen sowie Netzwerken Diese Kontrollen basieren auf Identitäten, melden Benutzer an bzw. ab und erteilen den Zugriff auf der Basis definierter Rollen", stellt Forrester fest.

Wenn Zero Trust die Zukunft ist, dreht sich zunächst alles um die Kontrolle darüber, wer sich im Netzwerk befindet, worauf Benutzer zugreifen und wie der Zugriff erfolgt. Mit diesen Fragen beschäftigt sich ZTNA und genau aus diesem Grund spielt diese Technologie eine zentrale Rolle bei der Zukunft der Cybersecurity.

Mehr erfahren unter
sophos.de/ztna

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

22-02-06 DE (MP)