LERNEN LEICHT GEMACHT

Palo Alto Networks Sonderausgabe

Zero Trust Network Access

für dummies®

Warum VPNs nicht mehr zeitgemäß sind

„True Least-Privilege"-Zugriff mit ZTNA 2.0

Die Einschränkungen veralteter ZTNA-Lösungen

Präsentiert von

paloalto® NETWORKS

Lawrence Miller

Über Palo Alto Networks

Palo Alto Networks ist das weltweit führende Unternehmen im Cybersicherheitsbereich. Wir entwickeln Innovationen, um Cyberbedrohungen stets einen Schritt voraus zu sein. So können Unternehmen Technologien mit Vertrauen nutzen. Wir bieten Tausenden von Kunden auf der ganzen Welt und in allen Branchen Cybersicherheitslösungen der nächsten Generation. Unsere erstklassigen Cybersicherheitsplattformen und -services werden von branchenführenden Bedrohungsdaten und modernster Automatisierung unterstützt. Ganz gleich, ob Sie unsere Produkte einsetzen, um Zero Trust in Ihrem Unternehmen umzusetzen, effektiv auf Sicherheitsvorfälle zu reagieren oder durch ein Partner-Ökosystem von Weltklasse bessere Sicherheitsergebnisse zu erzielen – wir setzen uns dafür ein, dass Ihre Technologie von Tag zu Tag sicherer wird. Das macht uns zum bevorzugten Cybersicherheitspartner zahlreicher Unternehmen.

Wir bei Palo Alto Networks sind bestrebt, die besten Mitarbeiter im Dienste unserer Mission zusammenzubringen. Deshalb sind wir stolz, als bevorzugter Arbeitgeber im Cybersicherheitsbereich anerkannt worden zu sein, unter anderem von Newsweek's Most Loved Workplaces (2021), Comparably Best Companies for Diversity (2021) und HRC Best Places for LGBTQ Equality (2022). Weitere Informationen finden Sie auf www.paloaltonetworks.com.

Zero Trust Network Access

für dummies®

Zero Trust Network Access

Palo Alto Networks Sonderausgabe

Lawrence Miller

für dummies®

Zero Trust Network Access für Dummies®, Sonderausgabe von Palo Alto Networks

Veröffentlicht von
John Wiley & Sons, Inc.
111 River St., Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-18374-6 (pbk); ISBN 978-1-394-18375-3 (ebk)

Allgemeine Informationen zu unseren sonstigen Produkten und Dienstleistungen oder zur Erstellung eines individuellen *Für Dummies*-Buches für Ihr Unternehmen oder Ihre Organisation erhalten Sie von unserer Abteilung Business Development in den USA telefonisch unter 877-409-4177 oder per E-Mail unter info@dummies.biz. Alternativ können Sie uns auch auf www.wiley.com/go/custompub besuchen. Für Informationen zur Lizenzierung der *Für Dummies*-Marke für Produkte oder Dienstleistungen kontaktieren Sie bitte BrandedRights&Licenses@Wiley.com.

Danksagung des Verlags

Die folgenden Personen haben bei der Erstellung dieses Buches mitgewirkt:

Project Editor: Elizabeth Kuball

Acquisitions Editor: Ashley Coffey

Editorial Manager: Rev Mengle

Client Account Manager: Cynthia Tweed

Production Editor: Magesh Elangovan

Weitere Unterstützung: Don Meyer, Shannon Bonfiglio

Inhaltsverzeichnis

Einführung

Die Arbeitswelt hat sich in relativ kurzer Zeit dramatisch verändert. Initiativen zur digitalen Transformation wie Remote-Arbeit und Cloud-Computing, die bereits vor der Coronapandemie im Gange waren, mussten plötzlich schneller umgesetzt werden, um den neuen Realitäten gerecht zu werden. Wir leben heute in einer Welt, in der „die Arbeit" kein Ort mehr ist, den Beschäftigte aufsuchen, sondern vielmehr eine Tätigkeit, die sie nahezu überall ausüben können.

Aufgrund dieses neuen Arbeitsparadigmas hat sich die Angriffsfläche von Unternehmen exponentiell vergrößert. Viele Architekturen unterstützen „Direct-to-App"-Verbindungen über das Internet, anstatt den Datenverkehr per Backhauling über private Netzwerke an Rechenzentren zu leiten. In einer Welt, in der sich viele Benutzer und Anwendungen außerhalb von Unternehmensnetzwerken und Rechenzentren befinden, funktionieren herkömmliche VPN-Verbindungen für den Fernzugriff nicht mehr. Veraltete Remote Access VPNs gewähren zu viel Zugriff und verfügen über wenige oder gar keine Funktionen zur Erkennung von Bedrohungen oder Schwachstellen, sodass zugangsbeschränkte Ressourcen durch die Kompromittierung von Benutzerkonten gefährdet sind. Da die Anzahl, das Ausmaß und Komplexität von Cyberangriffen ständig zunehmen, sind die meisten cloudfähigen Unternehmen heute mehr denn je bestrebt, ihre Sicherheitslücken zu schließen. Viele haben sich ZTNA-Lösungen (Zero Trust Network Access) zugewandt, um ihre Angriffsfläche zu reduzieren und ihre Unternehmen vor Ransomware und anderen Angriffen zu schützen.

Bestehende ZTNA-Lösungen (ZTNA 1.0) sind jedoch nicht mehr in der Lage, die Sicherheitsanforderungen heutiger Unternehmen zu erfüllen. Sie bieten zu viel Zugang und zu wenig Schutz, verfügen über uneinheitliche und unvollständige Sicherheitsfunktionen für web- und nicht webbasierte Anwendungen und lassen hinsichtlich Performance und Benutzerfreundlichkeit viel zu wünschen übrig. Aufgrund dieser Einschränkungen sind sie nicht in der Lage, die Flut der neuen und zunehmend komplexen Attacken auf wachsende Angriffsflächen zu bewältigen.

ZTNA 2.0-Lösungen sind der Königsweg in die Zukunft, da sie eine neue Ära des sicheren Datenzugriffs einleiten – in einer Welt, in der „die Arbeit" kein Ort mehr ist, sondern eine Tätigkeit.

Über dieses Buch

Zero Trust Network Access für Dummies, Palo Alto Networks-Sonderausgabe, besteht aus fünf Kapiteln, in denen die folgenden Themen behandelt werden:

- Die sich verändernde Sicherheitslandschaft, die Grundlagen von ZTNA und warum ZTNA 1.0 nicht mehr ausreicht (Kapitel 1)
- Wie ZTNA 2.0 die Einschränkungen bestehender ZTNA-Lösungen überwindet (Kapitel 2)
- Erfolgskritische Faktoren einer ZTNA 2.0-Lösung (Kapitel 3)
- Wichtige ZTNA 2.0-Anwendungsfälle und Erfolgsgeschichten von Kunden (Kapitel 4)
- Wichtige Fragen, die Sie Ihrem ZTNA-Anbieter stellen sollten (Kapitel 5)

Jedes Kapitel ist in sich geschlossen. Sie können deshalb einfach zu einem Thema springen, das Ihr Interesse weckt. Lesen Sie das Buch so, wie es Ihnen am liebsten ist (verkehrt herum oder rückwärts würden wir allerdings nicht empfehlen)!

Es gibt auch ein Glossar zum Nachschlagen von Abkürzungen und Begriffen.

Leichtfertige Annahmen

Einem Zitat zufolge haben die meisten unserer Annahmen ihre Nutzlosigkeit überlebt. Ich erlaube mir trotzdem, einige Annahmen zu treffen:

Ich gehe davon aus, dass Sie ein technischer Entscheidungsträger oder Praktiker sind und nach einer innovativen Lösung suchen, um Ihrer hybriden Belegschaft den sicheren Zugriff auf Daten zu ermöglichen. Ganz gleich, ob Sie ein Chief Information Security Officer (CISO), ein IT-Manager oder ein Netzwerk- oder Sicherheitsingenieur sind – dieses Buch zeigt Ihnen, wie Sie die Herausforderungen einer erheblich erweiterten Angriffsfläche und einer zunehmend feindlichen Bedrohungslandschaft mithilfe von ZTNA 2.0 bewältigen können.

In diesem Buch verwendete Symbole

In diesem Buch verwende ich gelegentlich bestimmte Symbole, um Ihre Aufmerksamkeit auf wichtige Informationen zu lenken. Sie werden auf die folgenden Hinweise stoßen:

Dieses Symbol macht auf wichtige Informationen aufmerksam, die Sie Ihrem nichtflüchtigen Speicher bzw. Ihren grauen Zellen anvertrauen sollten!

Dieses Symbol signalisiert, dass hier das Fachchinesisch hinter dem Fachchinesisch erläutert und etwas näher auf technische Details eingegangen wird.

Tipps sind immer willkommen – vor allem, wenn man nicht mit ihnen rechnet. Die Tipps in diesem Buch werden hoffentlich nützlich für Sie sein.

Dieses Symbol macht auf Dinge aufmerksam, vor denen Sie Ihre Mutter schon immer gewarnt hat. Doch auch wenn das nicht der Fall sein sollte, bieten Ihnen diese Abschnitte praktische Hinweise.

Zusätzliche Informationen

In diesem kurzen Buch kann ich natürlich nur eine Auswahl der wichtigsten Themen behandeln. Wenn Sie am Ende dieses Buches aber so beeindruckt sind, dass Sie unbedingt mehr erfahren wollen, gehen Sie einfach zu `www.paloaltonetworks.com/sase/ztna`.

IN DIESEM KAPITEL

- Die Sicherheitslandschaft im Wandel
- Die neue Arbeitswelt
- Die Grundlagen von Zero Trust
- Die Einschränkungen von ZTNA 1.0

Chapter 1
Die Sicherheitsauswirkungen der neuen Normalität

Dieses Kapitel beleuchtet moderne Sicherheitsherausforderungen, darunter die Zunahme von Bedrohungen, die Komplexität des Sicherheitsökosystems und die Talentlücke im Cybersicherheitsbereich. Außerdem wirft es einen Blick auf die Grundlagen von Zero Trust Network Access (ZTNA) und erläutert, warum Unternehmen ihre Fernzugriffsstrategien an neue Arbeitsmodelle anpassen müssen und sich nicht mehr auf herkömmliche Lösungen für die Zugriffskontrolle verlassen sollten.

Die Sicherheitslandschaft im Wandel

Die moderne Sicherheitslandschaft entwickelt sich ständig weiter, um mit den immer häufiger und komplexer werdenden Bedrohungen Schritt halten zu können. Um sich vor diesen Bedrohungen zu schützen, setzen viele Unternehmen ein kontinuierlich wachsendes Arsenal an punktuellen Sicherheitslösungen und -tools ein. Für die Verwaltung und den Betrieb dieser voneinander isolierten Tools sind jedoch häufig spezielle Fähigkeiten und Ressourcen erforderlich, über die die Sicherheitsteams der meisten Unternehmen einfach nicht verfügen.

Die zunehmende Häufigkeit und Komplexität von Bedrohungen

Datenschutzverletzungen und Ransomware-Angriffe sind mittlerweile so häufig, dass sie neben Wetter, Sport und Verkehr eigentlich ihre eigene Nachrichtenrubrik verdienen. Die Tatsache, dass Sicherheitsvorfälle heute alltäglich sind, macht sie jedoch nicht weniger gefährlich. Unternehmen, die ihren Sicherheitsstatus nicht ernst genug nehmen, riskieren große Schäden, falls es zu einem Angriff kommen sollte.


WARNUNG

Nach Angaben des Ponemon Institute stiegen die durchschnittlichen Kosten einer Datenpanne zwischen 2020 und 2021 um 10 Prozent auf 4,24 Millionen US-Dollar an. Dies war der größte jährliche Zuwachs der vergangenen sieben Jahre.

Leider führen die Sicherheitsteams vieler Unternehmen einen nahezu aussichtslosen Kampf gegen die immer perfider werdenden Taktiken, Techniken und Verfahren der Bedrohungsakteure.


ERINNERN

Um sich in der modernen Bedrohungslandschaft behaupten zu können, benötigen Unternehmen effektive Tools und ein Team kompetenter Sicherheitsanalysten. Leider ist eine ausgewogene Kombination aus Technologie und qualifizierten Experten für die meisten Unternehmen eher die Ausnahme als die Regel.

Zu viele Tools und zu viel Komplexität

Sicherheitsteams in Unternehmen setzen seit vielen Jahren spezialisierte Punktlösungen für bestimmte Sicherheitsherausforderungen und begrenzte Anwendungsfälle ein. Dieser Ansatz wird fälschlicherweise oft als eine Form der Tiefenverteidigung („Defense-in-Depth“) angesehen. Er hat jedoch zur Folge, dass das Sicherheitsökosystem mit zu vielen Tools überfrachtet ist, die die gesamte Betriebsumgebung komplex, kostspielig und ineffektiv machen. Laut einer IBM-Studie aus dem Jahr 2020 verwenden Unternehmen im Durchschnitt 45 Sicherheitstools. 30 Prozent setzen sogar mehr als 50 Tools ein. Aus dem in der Fachzeitschrift *InfoSecurity* zitierten *Panaseer 2022 Security Leaders Peer Report* geht sogar hervor, dass „die Umstellung auf Cloud- und Remote-Arbeit in den letzten zwei Jahren zu einer 19-prozentigen Zunahme der Anzahl von Sicherheitstools von 64 auf 76 geführt hat“.

Diese Sicherheitstools erzeugen täglich Tausende von Warnmeldungen – weit mehr, als ein Sicherheitsteam effektiv bewältigen kann.

Diese Warnmeldungen werden von vielen separaten Tools ausgegeben. Sicherheitsanalysten haben dann die Aufgabe, sie mühsam zueinander in Beziehung zu setzen (siehe Abbildung 1-1).

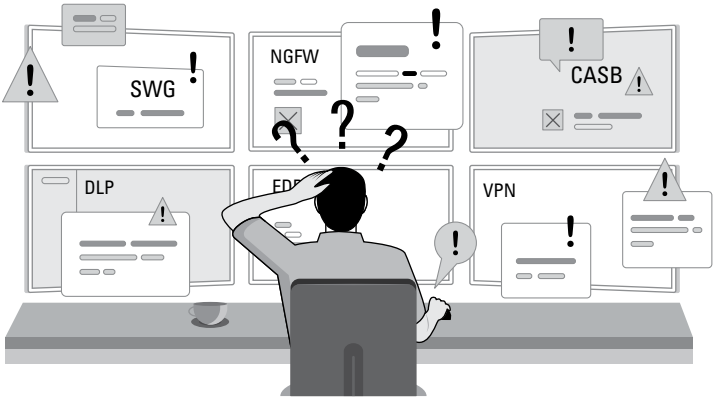

ABBILDUNG 1-1: Zu viele Sicherheitstools erhöhen die Komplexität der IT-Infrastruktur und führen zu Alarmmüdigkeit.

Fachkräftemangel und Talentlücke im Cybersicherheitsbereich

Neben der zunehmenden Häufigkeit und Komplexität von Bedrohungen und der wachsenden Zahl komplizierter Sicherheitstools in Unternehmen werden die Herausforderungen der modernen Sicherheitslandschaft noch durch ein weiteres Problem verschärft: den weltweiten Mangel an Fachkräften im Cybersicherheitsbereich. Schätzungen der Information Systems Audit and Control Association (ISACA) zufolge sind fast zwei Drittel der Sicherheitsteams in Unternehmen unterbesetzt und mehr als die Hälfte hat offene Stellen. Das International Information System Security Certification Consortium (ISC)² schätzt den weltweiten Mangel an Fachkräften für Cybersicherheit im Jahr 2021 auf 2,72 Millionen.

Warum Veränderungen nötig sind

Neben der sich schnell entwickelnden Bedrohungs- und Sicherheitslandschaft haben sich auch in der Arbeitswelt dramatische Veränderungen vollzogen. Da Benutzer heute von unterschiedlichen Geräten und Orten aus auf Anwendungen und Daten zugreifen, musste auch das Konzept des Vertrauens und die Kontrolle des Zugriffs auf diese Anwendungen und Daten neu überdacht werden.

Arbeit als Tätigkeit, nicht als Ort

Die Arbeitswelt hat sich dramatisch verändert. „Die Arbeit" ist heute nicht mehr nur ein Ort, den Beschäftigte aufsuchen, sondern vielmehr eine Tätigkeit, die sie ausüben. Wir gehen nicht mehr „zur Arbeit", sondern erledigen unsere Arbeit einfach an unterschiedlichen Orten. Für viele Unternehmen ist der Aufenthaltsort ihrer Mitarbeiter und der Ort, an dem sie ihre jeweiligen Arbeitsaufgaben ausführen, weitgehend irrelevant geworden. Viele Tätigkeiten lassen sich heute zu jeder Zeit und an jedem beliebigen Ort ausführen. Dieser Wandel wird durch zwei wichtige Trends vorangetrieben:

- **Anwendungen sind überall.** Die meisten Unternehmen sind zu einem Modell übergegangen, bei dem Anwendungen nicht mehr im eigenen Rechenzentrum ausgeführt werden. Das vorherrschende Bereitstellungsmodell für Anwendungen – einschließlich Software-as-a-Service (SaaS), Internet und Cloud – ist jetzt hybrid. Die überwältigende Mehrheit der Unternehmen nutzt heute eine Kombination aus Private Cloud, Public Cloud, Internet und SaaS.

  
  TIPP

  Laut dem *2021 State of the Cloud Report* von Flexera haben 80 Prozent der Unternehmen heute eine Hybrid-Cloud-Strategie. Statista berichtet, dass das durchschnittliche Unternehmen 110 SaaS-Anwendungen nutzt.

- **Benutzer sind überall.** Viele Unternehmen verwenden heute ein hybrides Arbeitsmodell, das *teilweise Fernarbeit* (zwei bis drei Tage pro Woche im Homeoffice), vollständige Fernarbeit oder andere flexible Arrangements unterstützt. Dieser Trend wurde durch die Covid-19-Pandemie stark beschleunigt, und als Unternehmen die positiven Auswirkungen dieses Modells auf die Produktivität und Arbeitsmoral ihrer Mitarbeiter erkannten, wurde es in der Arbeitswelt schnell zur neuen Normalität.

  
  TIPP

  Laut dem Bericht *State of Hybrid Workforce Security 2021* von Palo Alto Networks möchten 76 Prozent der Mitarbeiter auch nach der Pandemie weiterhin hybride Arbeitsformen nutzen.

Dieser Wandel bringt jedoch einige wichtige Auswirkungen auf die IT und die Sicherheit mit sich.

Früher war die Remote-Belegschaft von Unternehmen mit Rechenzentren verbunden. Dabei war der Zugriff auf die Anwendungen im Rechenzentrum sowie auf Internet- und SaaS-Anwendungen geschützt. Dies wurde durch den Einsatz unterschiedlicher punktueller Sicherheitstools am Perimeter des Rechenzentrums erreicht: Firewalls, Proxys, Intrusion Prevention Systems (IPS), Cloud Access

Security Broker (CASB), Anti-Malware-Produkte, DNS-Security-Tools (Domain Name System) usw.

Bei diesem Modell bauten Unternehmen ihre Wide Area Networks (WANs) mit Multiprotocol Label Switching (MPLS) und anderen dedizierten Verbindungen auf, die die Zweigstellen mit dem Rechenzentrum verbanden. Der gesamte ins Internet gehende Verkehr wurde durch das Rechenzentrum geleitet. Dadurch konnte der riesige Sicherheitsstack des Unternehmens zentralisiert und der gesamte Traffic durch ihn hindurchgeleitet werden (siehe Abbildung 1-2).

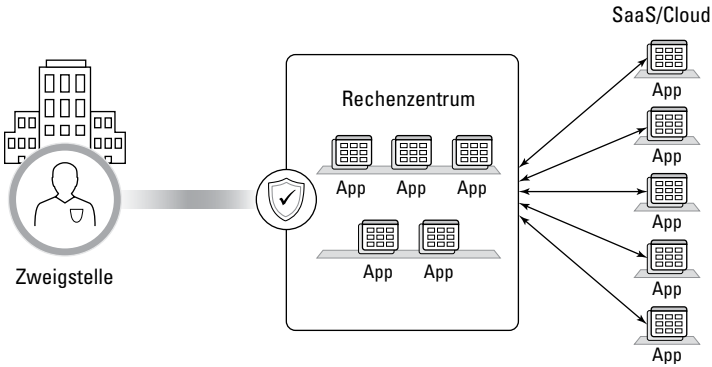

ABBILDUNG 1-2: Als die Arbeit noch jeden Tag am selben Ort stattfand, war es relativ einfach, Sicherheit zu gewährleisten.

Jetzt haben wir ein völlig anderes Modell.

Benutzer, Anwendungen und Daten sind überall

Unternehmen haben ihre WAN-Architektur umgestellt, um Remote-Mitarbeiter direkt mit dem Internet anstatt mit dem Rechenzentrum zu verbinden. Sie müssen Benutzern überall – am Hauptsitz und in Zweigstellen, im Homeoffice und über mobile Geräte – einen sicheren und zuverlässigen Zugang zu Anwendungen und Daten bieten, die sich überall befinden können – in Rechenzentren, Private Clouds, Public Clouds und SaaS-Anwendungen.

Benutzer verbinden sich jetzt direkt mit allen Anwendungen, die sie für die Arbeit benötigen (siehe Abbildung 1-3). Der Speicherort der Anwendung ist weniger wichtig; was jetzt zählt, ist die Bereitstellung einer konsistenten, optimierten und sicheren Benutzererfahrung beim Zugriff auf all diese Anwendungen.

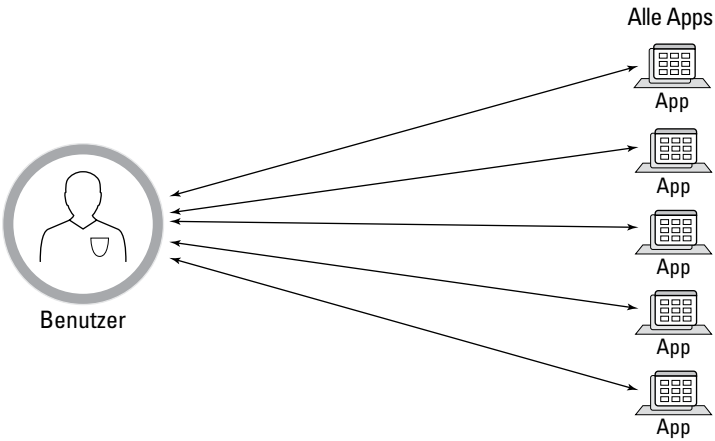

ABBILDUNG 1-3: Benutzer verbinden sich heute direkt mit ihren Anwendungen.

„Direct-to-App"-Konnektivität vergrößert die Angriffsfläche exponentiell

Die direkte Verbindung zu Anwendungen stellt eine dramatische Veränderung gegenüber dem herkömmlichen Modell dar, durch die sich die Angriffsfläche für Unternehmen exponentiell vergrößert. Je größer die Angriffsfläche wird, desto dringender werden effektive Sicherheits- und Zugriffskontrollen für den Schutz von Unternehmensanwendungen und -daten benötigt (siehe Abbildung 1-4).

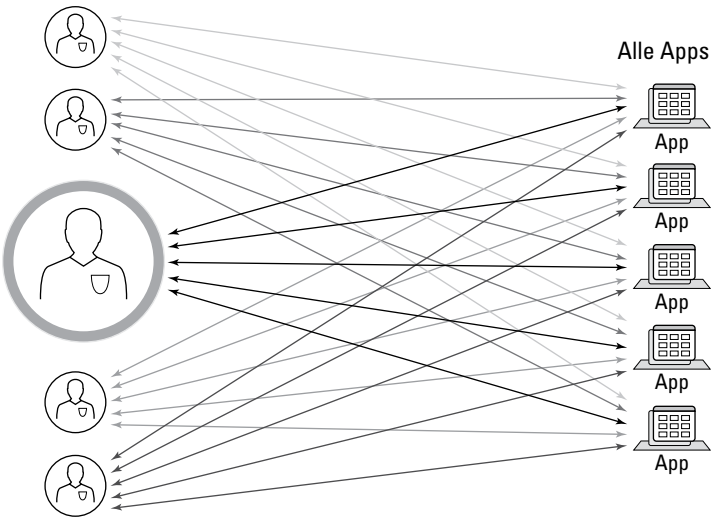

ABBILDUNG 1-4: Die Angriffsfläche hat sich drastisch vergrößert.

VPNs sind nicht granular genug

Virtual Private Networks (VPNs) wurden entwickelt, um Remote-Mitarbeitern einen sicheren Zugriff auf ein Local Area Network (LAN) oder ein Subnetz im LAN zu ermöglichen. Die Verbindung mit dem Unternehmensnetzwerk erfolgt dabei über einen privaten, verschlüsselten Tunnel. Das klingt wie eine brauchbare Lösung, doch leider fehlt es VPNs an Flexibilität und Granularität, um den Datenverkehr effektiv zu kontrollieren und genau zu überwachen, was Benutzer tun dürfen und auf welche Anwendungen sie zugreifen können. Ein Benutzer, dem der Zugriff auf eine Ressource gewährt wurde, kann auf alles im Netzwerk oder Subnetz zugreifen, was zwangsläufig zu Sicherheitslücken und Problemen bei der Durchsetzung von Richtlinien führt.

Im Gegensatz dazu sorgt ZTNA für einen sicheren Fernzugriff auf Anwendungen, da der Ansatz auf granularen Zugriffskontrollrichtlinien basiert. Benutzer können nur auf autorisierte Anwendungen zugreifen, während bei VPNs nach der Überprüfung alles zugänglich ist. ZTNA basiert auf dem Prinzip der geringsten Berechtigungen (Least-Privilege-Prinzip), um die Angriffsfläche drastisch zu reduzieren und den allgemeinen Sicherheitsstatus des Unternehmens zu verbessern.

Was ist Zero Trust Network Access?

ZTNA ist eine Produktkategorie, die den sicheren Fernzugriff auf Anwendungen und Services auf der Grundlage definierter Zugriffskontrollrichtlinien ermöglicht. ZTNA-Lösungen verweigern grundsätzlich den Zugriff auf eine Anwendung oder einen Service, es sei denn, er wurde dem Benutzer ausdrücklich gewährt. Da die Anzahl der Remote-Benutzer, die Netzwerkzugriff benötigen, voraussichtlich weiter zunehmen wird, sollten Unternehmen genau wissen, welche Sicherheitslücken und Vorteile mit ZTNA-Lösungen verbunden sind.

ERINNERN

ZTNA ist ein wichtiger Bestandteil der Zero Trust-Philosophie „niemals vertrauen, immer überprüfen“, die von Forrester entwickelt wurde, um dem Bedarf nach einem besseren Schutz von Daten Rechnung zu tragen. Bei ZTNA müssen sich Benutzer über einen Gateway-Broker authentifizieren, bevor sie Zugriff auf die benötigten Anwendungen erhalten. Auf diese Weise können Benutzer identifiziert und Richtlinien erstellt werden, um den Zugriff auf Ressourcen einzuschränken, Datenverluste zu minimieren und eventuell auftretende Probleme oder Bedrohungen schnell zu entschärfen.

Die Grundlagen von ZTNA

Mit ZTNA erhalten Benutzer erst dann Zugriff auf die gewünschten Ressourcen, wenn sie durch den Access Broker authentifiziert wurden. Der ZTNA-Service bietet dem Benutzer dann über einen sicheren, verschlüsselten Tunnel Zugriff auf die Anwendung. Auf diese Weise erhalten Unternehmensanwendungen und -services eine zusätzliche Schutzebene, da IP-Adressen (Internet Protocol), die ansonsten öffentlich sichtbar wären, abgeschirmt werden.

Wie Software-Defined Perimeters (SDPs) verwendet auch ZTNA das Konzept einer „Dark Cloud", d. h., unbefugte Benutzer können keine Anwendungen und Services sehen, auf die sie keinen Zugriff haben. Dies schützt vor lateralen Bewegungen, bei denen Angreifer einen kompromittierten Endpunkt oder Zugangsdaten nutzen, um andere Services zu durchsuchen und anzugreifen.

ZTNA 1.0

Frühere Versionen von ZTNA – ZTNA 1.0-Lösungen – wurden zu einer Zeit eingeführt, als die Bedrohungslandschaft, die Arbeitswelt und die Unternehmensnetzwerke völlig anders aussahen als heute. ZTNA 1.0 wird diesen veränderten Gegebenheiten nicht mehr gerecht, sodass böswillige Akteure heute leicht neue Wege finden können, um die Schwachstellen von ZTNA 1.0-Lösungen auszunutzen.

ZTNA 1.0 wurde mit dem Ziel entwickelt, Unternehmen durch die Begrenzung ihrer Risiken und die Reduzierung ihrer Angriffsfläche zu schützen. Um Benutzern die Verbindung zu einer Anwendung zu erleichtern, setzt ZTNA 1.0 einen Access Broker ein. Wenn ein Benutzer auf eine Anwendung zugreifen will, bestimmt der Access Broker, ob der Benutzer tatsächlich eine Zugriffsgenehmigung hat. Nachdem die Genehmigung überprüft wurde, gewährt der Access Broker dem Benutzer Zugriff auf die gewünschte Anwendung, und die Verbindung wird hergestellt (siehe Abbildung 1-5).

Das ist alles. Danach ist der Broker nicht mehr im Spiel, und der Benutzer erhält vollständigen Zugriff auf die gewünschte Anwendung, ohne weiter durch das Sicherheitssystem überwacht zu werden.

Dieser „Zulassen-und-Ignorieren"-Ansatz ist das Architekturmodell von ZTNA 1.0. Im Kontext der heutigen Bedrohungslandschaft ist dieses Modell nicht nur problematisch – es ist geradezu gefährlich.

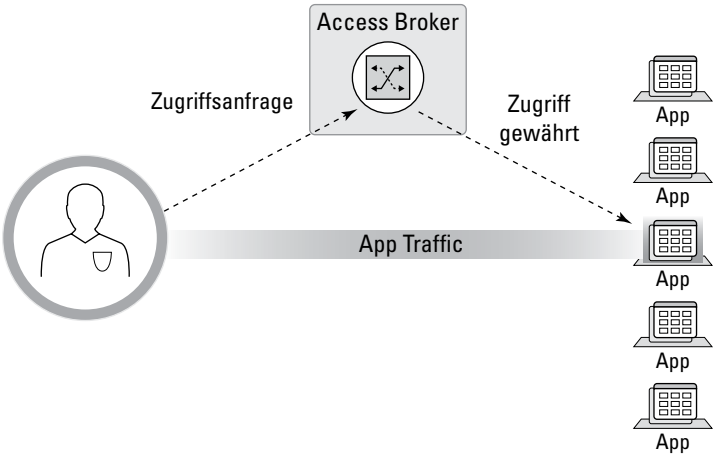

ABBILDUNG 1-5: Mit ZTNA 1.0 versuchte die Branche, das Problem des sicheren Zugriffs zu lösen.

ZTNA 1.0 weist in der heutigen Umgebung erhebliche Sicherheitsmängel auf

Viele ZTNA-Produkte basieren auf SDP-Architekturen, die keine Inhaltsprüfung bieten, was zu Diskrepanzen zwischen den für die einzelnen Anwendungen verfügbaren Schutzmechanismen führt. Um einen durchgängigen Schutz zu gewährleisten, sind neben dem ZTNA-Modell zusätzliche Kontrollen und eine Überprüfung des gesamten Datenverkehrs aller Anwendungen erforderlich. Neben diesen Herausforderungen gibt es im Zusammenhang mit ZTNA 1.0-Lösungen fünf wesentliche Probleme, die die Effektivität dieses Ansatzes in der sich schnell entwickelnden Sicherheitslandschaft und Arbeitswelt von heute einschränken.

Verstößt gegen das Least-Privilege-Prinzip

Das Prinzip der geringsten Berechtigungen (Least Privilege) schreibt vor, dass ein Benutzer nur minimale Zugriffsrechte auf eine Anwendung oder Ressource erhalten darf: nämlich nur die, die er zur Ausführung einer genehmigten Aufgabe wirklich benötigt – und nicht

mehr. Eine „Zero Trust"-Strategie setzt voraus, dass keine Anwendung, kein Gerät und kein Benutzer, die bzw. der sich mit einer Netzwerkanwendung oder -ressource zu vernetzen, grundsätzlich vertrauenswürdig ist.

Bestehende ZTNA 1.0-Lösungen verwalten den Anwendungszugriff auf Layer 3 (Network) und Layer 4 (Transport) des Open Systems Interconnection (OSI)-Modells und verwenden dabei nur IP-Adressen und Portkonstruktionen gemäß TCP (Transmission Control Protocol) und UDP (User Datagram Protocol).

Obwohl Netzwerke keine Anwendungen sind, verlassen sich ZTNA 1.0-Lösungen auf Zugriffskontrollen auf Netzwerkebene, um Benutzern Zugriff auf Anwendungsebene zu gewähren. Die Verwendung von auf Layer 3 und 4 definierten Richtlinien führt leider zu einer Reihe von Problemen. Wenn eine Anwendung zum Beispiel dynamische Ports oder IP-Adressen verwendet, müssen Sie Zugriff zu einem größeren Bereich von IP-Adressen und Ports Zugriff gewähren, wodurch das Unternehmen mehr Risiken ausgesetzt wird. Es ist auch nicht möglich, den Zugriff auf die Ebene einer Teilanwendung oder Anwendungsfunktion zu beschränken – er kann immer nur vollständigen Anwendungen gewährt werden. Dadurch erhalten Benutzer weitaus mehr als den gewünschten oder beabsichtigten Zugriff (siehe Abbildung 1-6).

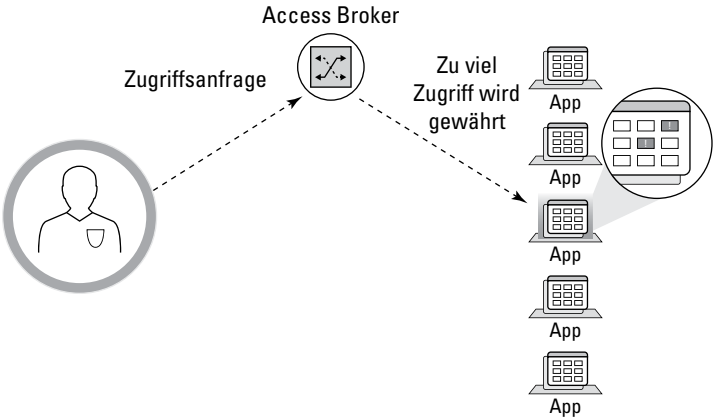

ABBILDUNG 1-6: ZTNA 1.0 verstößt gegen das Least-Privilege-Prinzip.

WARNUNG

Jede Malware, die auf denselben IP-Adressen und Portnummern wie erlaubte Anwendungen „mithört“, kann ungehindert mit der C2-Infrastruktur (Command-and-Control) kommunizieren und sich lateral ausbreiten.

Stützt sich auf ein „Zulassen-und-Ignorieren“-Modell

Eine weitere Einschränkung von ZTNA 1.0-Lösungen besteht darin, dass sie auf dem riskanten Modell „Zulassen und Ignorieren“ basieren (siehe Abbildung 1-7). Wenn der Access Broker eine Verbindung zwischen einem Benutzer und einer Anwendung herstellt, wird der Benutzer- und Gerätedatenverkehr als vertrauenswürdig eingestuft und für die Dauer der Sitzung werden keine weiteren Überprüfungen durchgeführt.

Die Annahme, dass Vertrauen nur einmal und dann nie wieder überprüft werden muss, ist der sicherste Weg in eine Katastrophe. Auch nachdem einem Akteur Vertrauen gewährt wurde, kann noch eine Menge passieren. Das Verhalten von Benutzern und Anwendungen kann sich ändern, und Anwendungen können kompromittiert werden.

WARNUNG

Viele moderne Bedrohungen nutzen erlaubte Aktivitäten aus, um keinen Alarm auszulösen.

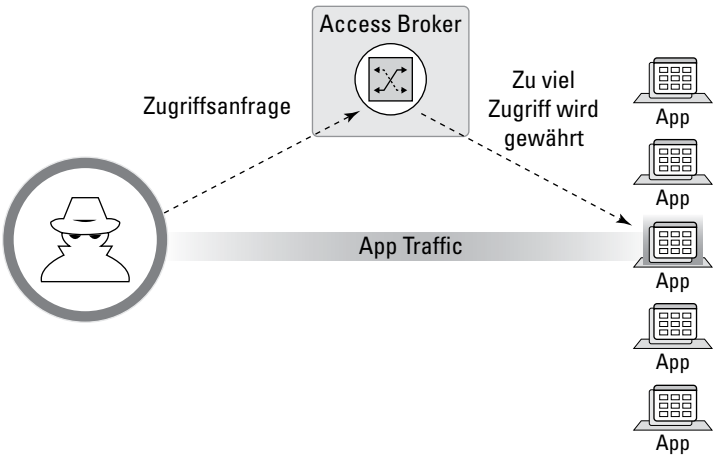

ABBILDUNG 1-7: ZTNA 1.0: Zulassen und ignorieren.

Führt keine Sicherheitsüberprüfung durch

ZTNA 1.0-Lösungen überprüfen auch nicht den Anwendungsdatenverkehr (siehe Abbildung 1-8). Wenn eine Verbindung hergestellt wurde, vertraut ZTNA 1.0 dieser aktiven Sitzung implizit und führt daher keine weitere Überprüfung des Datenverkehrs durch. Wenn das Gerät kompromittiert ist und Malware in die Sitzung eingeschleust wird, gibt es für eine ZTNA 1.0-Lösung keine Möglichkeit, bösartigen oder anderweitig kompromittierten Datenverkehr zu erkennen und entsprechend zu reagieren.

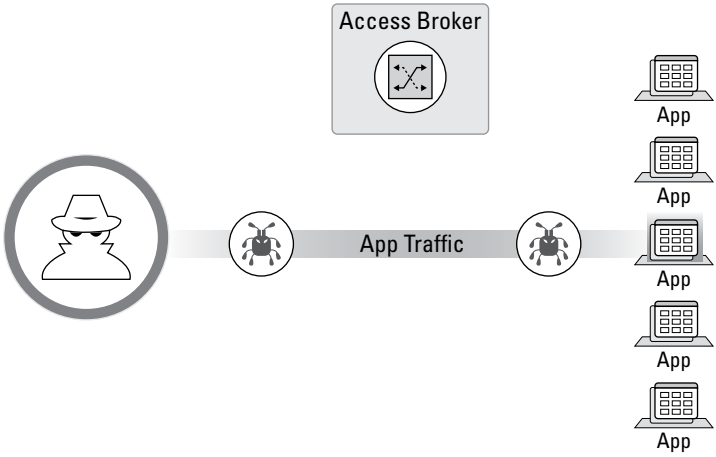

ABBILDUNG 1-8: ZTNA 1.0 bietet keine Sicherheitsüberprüfungen.

Schützt nicht alle Daten

ZTNA 1.0-Lösungen bieten keine ausreichende Sicherheit für Daten – vor allem nicht für die Daten privater Anwendungen (siehe Abbildung 1-9). Dadurch ist ein großer Teil des Datenverkehrs des Unternehmens dem Risiko der Datenexfiltration durch böswillige Insider oder externe Angreifer ausgesetzt. Außerdem erfordert dieser Ansatz zusätzliche DLP-Lösungen (Data Loss Prevention), um sensible Daten in privaten Anwendungen (anstatt SaaS-Anwendungen) zu schützen. Durch ZTNA 1.0 werden mehr Komplexität und Risiken eingeführt, da Unternehmen mehrere Einzelprodukte einsetzen müssen, um ihre Daten überall zu schützen.

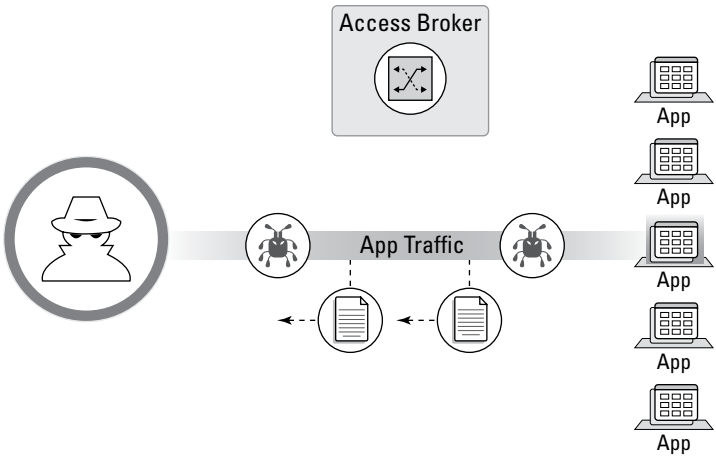

ABBILDUNG 1-9: ZTNA 1.0 bietet keine Datensicherheit.

Es werden nicht alle Anwendungen geschützt

Außerdem schützen ZTNA 1.0-Lösungen nicht alle Anwendungen (siehe Abbildung 1-10). Sie unterstützen keine cloudbasierten oder anderen Anwendungen, die dynamische Ports verwenden, oder serverbasierte Anwendungen wie Helpdesk-Support-Anwendungen, die serverbasierte Verbindungen zu Remote-Geräten nutzen. ZTNA 1.0-Lösungen unterstützen auch keine SaaS-Anwendungen.

Moderne cloudnative Anwendungsstacks bestehen aus zahlreichen Containern und Microservices, die häufig dynamische IP-Adressen und Portnummern verwenden. Die ZTNA 1.0-Zugriffskontrolle ist in diesen Umgebungen völlig unwirksam, da der Zugriff für breite Bereiche von IP-Adressen und Ports geöffnet werden muss, was dem Prinzip von Zero Trust zuwiderläuft.

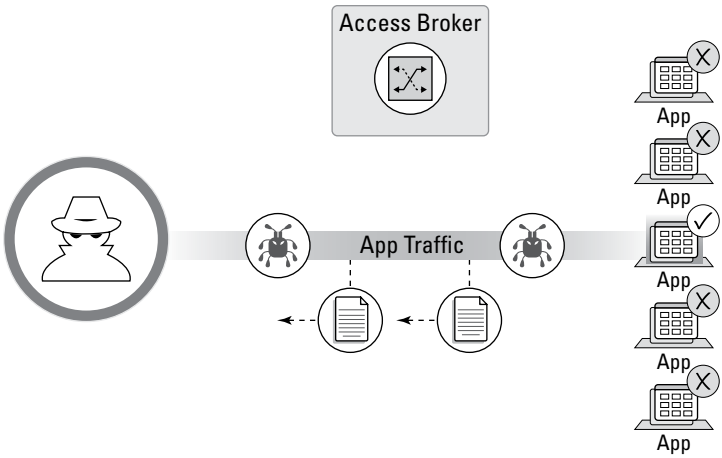

ABBILDUNG 1-10: ZTNA 1.0 kann nicht alle Anwendungen schützen.

Je mehr Unternehmen den Weg in die Cloud antreten und cloudnative Anwendungen nutzen, desto ungebräuchlicher wird ZTNA 1.0.

TIPP

Bei so vielen Einschränkungen werden Sie sich vielleicht fragen, wie es ZTNA 1.0 überhaupt auf den Markt geschafft hat. Vergessen Sie nicht, dass ZTNA 1.0 vor etwa zehn Jahren eingeführt wurde; als die Welt noch ganz anders aussah. Vor ZTNA 1.0 war eigentlich nur ein VPN-Zugang erforderlich, da sich alle Anwendungen im Rechenzentrum befanden und die meisten Benutzer im Büro arbeiteten. ZTNA 1.0 wurde eingeführt, um einige der mit VPNs verbundenen Probleme zu lösen, als sich Benutzer und Anwendungen immer mehr von der Unternehmenszentrale und dem Rechenzentrum entfernten. Heute, in einer Welt mit hybriden Netzwerkumgebungen und hybriden Belegschaften – in der Arbeit eher eine Tätigkeit als ein Ort ist und Anwendungen und Benutzer sich praktisch überall befinden können –, ist eindeutig ein neuer Ansatz nötig. Kapitel 2 erklärt, wie ZTNA 2.0 über die Grenzen von ZTNA 1.0 hinausgeht, um moderne Sicherheitsherausforderungen zu bewältigen.

IN DIESEM KAPITEL

- Umsetzung des Least-Privilege-Zugriffs
- Kontinuierliche Überprüfung des gewährten Vertrauens
- Kontinuierliche Sicherheitsprüfung
- Schutz aller Daten
- Kontrolle und Schutz des Anwendungszugriffs

Kapitel 2
Zero Trust Network Access (ZTNA) 2.0

Veraltete Lösungen für den sicheren Fernzugriff und überholte Architekturen – wie Virtual Private Networks (VPNs) und die erste Version von Zero Trust Network Access (ZTNA) – sind nicht mehr in der Lage, die Flut neuer und zunehmend komplexer Cyberangriffe auf immer größer werdenden Angriffsflächen zu bewältigen. Eines steht folglich fest: Wir brauchen einen neuen Ansatz. Dieses Kapitel stellt ZTNA 2.0 vor und erläutert, wie die Lösung moderne Sicherheitsherausforderungen angeht und die Einschränkungen früherer Ansätze überwindet, um einen sicheren Fernzugriff für die hybriden Belegschaften von heute zu gewährleisten.

Vollständige Umsetzung des Least-Privilege-Zugriffs

ZTNA 2.0 verwendet zustandsbehaftete Funktionen zur Identifizierung von Anwendungen, Benutzern und Geräten zur Umsetzung des Least-Privilege-Zugriffs (siehe Abbildung 2-1).

Anwendungen werden auf Layer 7 (Application) des Open Systems Interconnection (OSI)-Modells identifiziert. Diese Schicht geht über Low-Level-Netzwerkkonstrukte wie Layer 3 (Network [IP-Adresse]) und Layer 4 (Transport [Port oder Protokoll]) hinaus. Die

Identifizierung erfolgt, indem Informationen über TCP-Sitzungen (Transmission Control Protocol), Anwendungs-Handshakes, Anwendungsverhalten, zustandsbehaftete Protokolle usw. kontinuierlich erfasst werden.

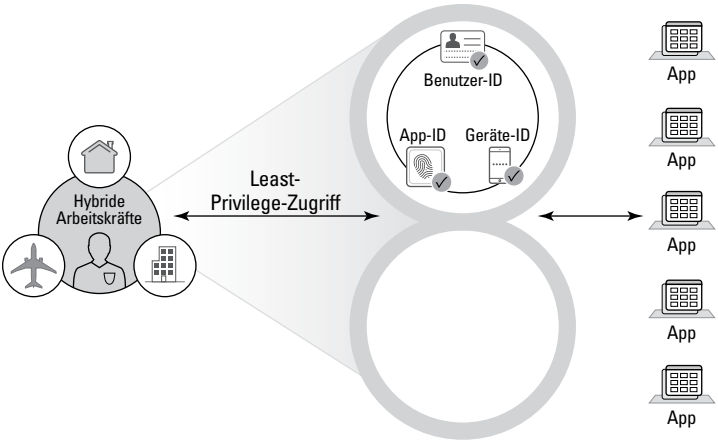

ABBILDUNG 2-1: ZTNA 2.0 verwendet die Anwendungs-, Benutzer- und Geräte-ID, um den Least-Privilege-Zugriff umsetzen.

Durch diesen Einblick in Anwendungen, insbesondere moderne Microservices-Anwendungen, kann ZTNA 2.0 fein abgestufte Kontrollen bereitstellen und verhindern, dass Sub-App-Funktionen oder andere Kommunikationsschemata offengelegt werden, auf die Benutzer keinen Zugriff benötigen. Gleichzeitig werden durch die Kontrolle der Benutzer- und Geräte-ID kontinuierlich Informationen über Benutzer und ihre Geräte erfasst. Die Kombination von Anwendungs-, Benutzer- und Geräteidentifikation geht über einfache punktuelle Vertrauensgarantien (wie in ZTNA 1.0) hinaus und schafft eine Umgebung, in der umfangreiche, kontextbezogene Informationen für eine bessere Entscheidungsfindung bei der Zugriffskontrolle bereitgestellt werden können. Mit ZTNA 2.0 können Unternehmen jedem Benutzer auf jedem Gerät Zugriff auf die von ihm angeforderte Anwendung gewähren und kontinuierlich weitere Kontextinformationen erfassen. Dadurch ist es möglich, in Echtzeit auf Änderungen zu reagieren, die Angriffsfläche erheblich zu reduzieren und gleichzeitig wahren „Least-Privilege"-Zugriff durchzusetzen.

Kontinuierliche Überprüfung des gewährten Vertrauens

Das Kernprinzip von Zero Trust besteht darin, implizites Vertrauen aus der Gleichung zu nehmen – das heißt: „Niemals vertrauen, immer überprüfen“. Ohne eine Funktion zur kontinuierlichen Vertrauensüberprüfung muss das System jedoch davon ausgehen, dass sich ein Benutzer, ein Gerät oder eine Anwendung auf unbestimmte Zeit vertrauenswürdig verhalten wird, nachdem eine Verbindung hergestellt wurde. Die Vertrauenswürdigkeit kann allerdings auch nach der Gewährung des Zugriffs beeinträchtigt werden, z. B. durch Änderungen im Verhalten des Benutzers, des Geräts oder der Anwendung, oder durch eine Sicherheitsgefährdung.

Durch die kontinuierliche Vertrauensüberprüfung, die ein Bestandteil von ZTNA 2.0 ist, werden der Zustand des Geräts, alle Änderungen daran sowie das Benutzer- und Anwendungsverhalten ständig überwacht und kontrolliert, um bei Bedarf in Echtzeit reagieren zu können (siehe Abbildung 2-2).

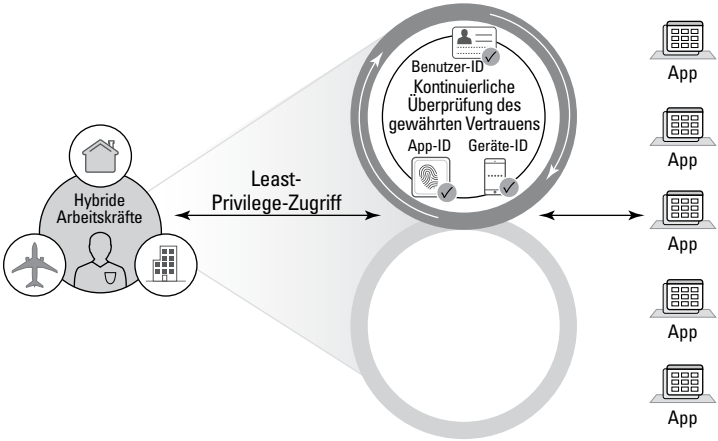

ABBILDUNG 2-2: Durch die kontinuierliche Vertrauensüberprüfung wird das Verhalten des Geräts, der Anwendung und des Benutzers ständig überwacht, auch wenn der Benutzer bereits Zugriff auf die Anwendung erhalten hat.

Kontinuierliche Sicherheitsprüfung

ZTNA 2.0 bietet eine kontinuierliche Sicherheitsprüfung mit Threat Intelligence, fortschrittlicher Uniform Resource Locator (URL)-Filterung, Bedrohungsabwehr, Software-as-a-Service (SaaS)-Sicherheit, Domain Name System (DNS)-Sicherheit und mehr. Deep Packet Inspection (DPI) und Funktionen zur kontinuierlichen Sicherheitsüberprüfung nutzen auch Technologien zur Bedrohungsabwehr, die auf künstlicher Intelligenz (KI) und maschinellem Lernen (ML) basieren, um Zero-Day-Bedrohungen direkt zu stoppen (siehe Abbildung 2-3).

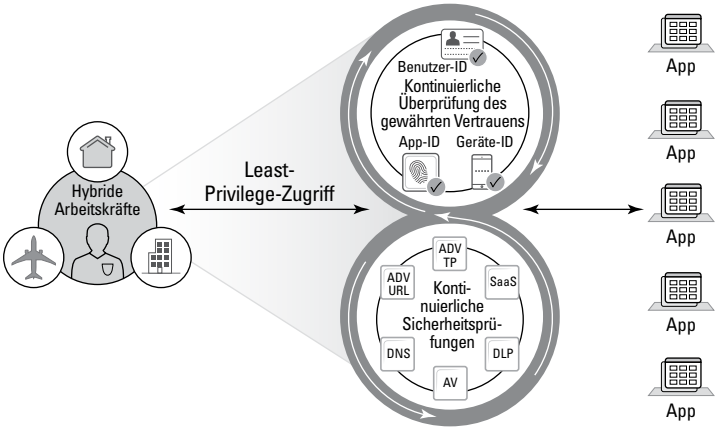

ABBILDUNG 2-3: Durch kontinuierliche Sicherheitsüberprüfungen wird Ihre Umgebung überwacht, um sie vor Bedrohungen zu schützen.

Schutz aller Daten

ZTNA 2.0 wendet fortschrittliche Data Loss Prevention (DLP)-Funktionen konsistent auf alle Anwendungsdaten an. Dabei werden immer dieselben DLP-Richtlinien durchgesetzt, unabhängig davon, ob sich die Daten in einer benutzerdefinierten Anwendung, einer SaaS-Anwendung, einer Webanwendung, einem öffentlichen Repository oder einer Datenbank befinden. Es wird einfach immer davon ausgegangen, dass die betreffenden Anwendungen zu schützen sind. Unternehmen können mit einer einzigen Lösung rigorose Datenschutz- und Sicherheitsrichtlinien für alle ihre Anwendungen durchsetzen (siehe Abbildung 2-4).

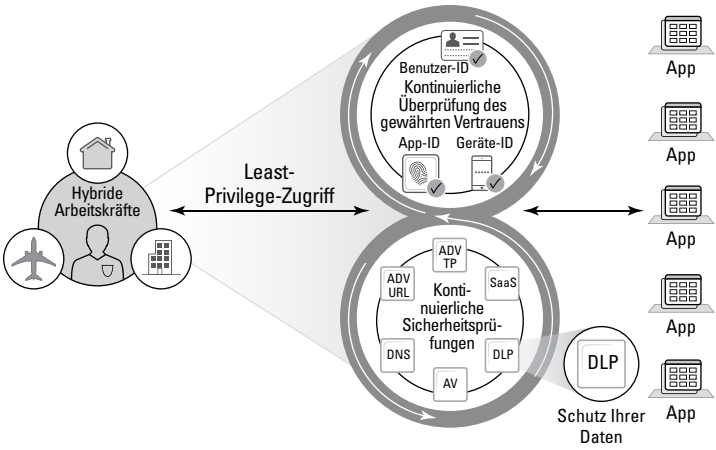

ABBILDUNG 2-4: Dieselben strikten Datenschutz- und Sicherheitsrichtlinien werden zur Gewährleistung der Datensicherheit durchgehend in der gesamten Umgebung angewendet.

Schutz aller Anwendungen

ZTNA 2.0 bietet durchgehende Sicherheit für alle Anwendungen im Unternehmen. Dabei kann es sich um moderne cloudnative Anwendungen auf Basis von Microservices handeln, die nicht durch IP-Adressen und Ports eingeschränkt sind, oder um SaaS-Anwendungen, benutzerdefinierte oder Legacy-Anwendungen (siehe Abbildung 2-5).

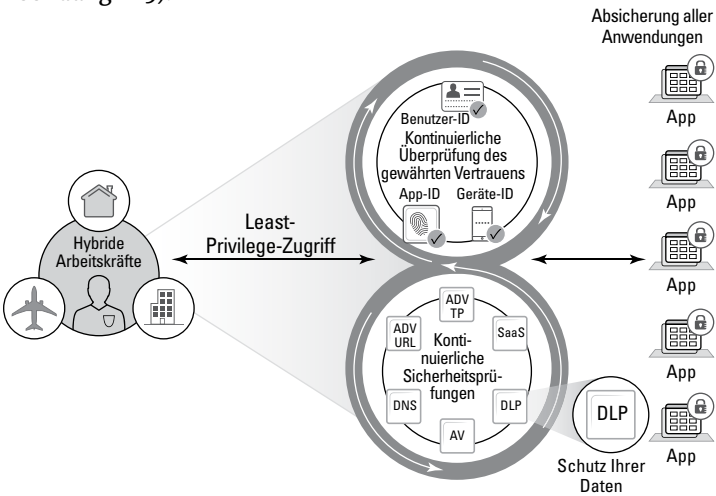

ABBILDUNG 2-5: ZTNA 2.0 bietet konsistente Sicherheit für alle Anwendungen – ob cloud-nativ, SaaS, benutzerdefiniert oder Legacy.

ERINNERN

ZTNA 2.0 überwindet die Einschränkungen von ZTNA 1.0-Lösungen und bietet bessere Sicherheitsergebnisse. Damit unterstützt die Lösung die digitale Transformation und die Anforderungen hybrider Belegschaften, denen sich Unternehmen heute stellen müssen. Die fünf Grundprinzipien von ZTNA sind:

- **Least Privilege:** Gewährleistet die strengste Durchsetzung des Least-Privilege-Prinzips und bietet Zugriffskontrolle von Layer 3 (Network) bis Layer 7 (Application), um die Angriffsfläche drastisch zu reduzieren.
- **Kontinuierliche Überprüfung des gewährten Vertrauens:** Wenn sich das Verhalten eines Benutzers, einer Anwendung oder eines Geräts ändert, muss es eine kontinuierliche Bewertung des gewährten Vertrauensniveaus und die Möglichkeit geben, auf alle Änderungen angemessen und in Echtzeit zu reagieren.
- **Kontinuierliche Sicherheitsprüfungen:** Der gesamte Datenverkehr wird kontinuierlich überwacht, um das Unternehmen vor allen Bedrohungen – einschließlich Advanced Persistent Threats (APTs) und Zero Days – und allen Angriffsvektoren zu schützen.
- **Datensicherheit:** Alle Daten werden durch Richtlinien geschützt, die konsistent auf alle Anwendungsdaten angewendet werden – von den Daten in Anwendungen auf Legacy-Mainframes bis hin zu Daten in modernen, cloudnativen und Collaboration-Anwendungen.
- **Durchgehende Sicherheit für alle Anwendungen:** Alle Anwendungen im gesamten Unternehmen – einschließlich benutzerdefinierter Anwendungen, Cloud-nativercloudnativer Anwendungen und SaaS-Anwendungen – werden geschützt und gesichert.

IN DIESEM KAPITEL

- die Bedeutung einer außergewöhnlichen Benutzererfahrung
- Bereitstellung einer einfachen, einheitlichen Lösung

Kapitel 3
Erfolgskritische Fähigkeiten von ZTNA 2.0-Lösungen

Dieses Kapitel erklärt, warum eine außergewöhnliche Benutzererfahrung und eine einheitliche Lösung so wichtig für die erfolgreiche Einführung Ihrer ZTNA 2.0-Lösung sind.

Schaffung einer außergewöhnlichen Benutzererfahrung

Wenn Sie Ihre Benutzer fragen, was sie von den Sicherheitstools Ihres Unternehmens halten, werden Sie die Worte „Ich liebe die Benutzererfahrung!“ wahrscheinlich eher selten zu hören bekommen.“ Sicherheitstools sind nicht nur komplex und notorisch schwer zu bedienen, sondern verlangsamen auch die Arbeitsprozesse von Benutzern. Anti-Malware-Scans nehmen viel wertvollen Arbeitsspeicher in Anspruch und machen ihre Computer langsamer. Durch die Verbindung zum Virtual Private Network (VPN) verlangsamt sich der Internetzugang, während sich die Latenzzeit der Anwendungen erhöht. Dies führt dazu, dass viele Benutzer die Sicherheitskontrollen, die sie vor sich selbst schützen sollen, auf kreative Weise umgehen.

Bei den derzeit eingesetzten ZTNA-1.0 Lösungen verhält es sich nicht anders. Sie verlassen sich auf physische Geräte in Colocation-Einrichtungen, die lose miteinander verbunden sind und nutzen das öffentliche Internet als Backbone. Dadurch sind diese Lösung nicht nur hinsichtlich ihrer Reichweite, Skalierbarkeit und Leistung erheblich eingeschränkt, sondern auch zu sehr von den Rechenzentren Dritter und von nicht optimalen Verbindungen abhängig. Sie bieten auch keine echte Mandantenfähigkeit, um Probleme wie „laute Nachbarn“ und „Fate-Sharing“ zu mindern. So müssen Kunden Abstriche in puncto Sicherheit in Kauf nehmen, um die gewünschte Benutzererfahrung zu erhalten.

Um eine gleichbleibend hohe Leistung zu gewährleisten, sollten ZTNA 2.0-Lösungen für jeden Kunden eine eigene Datenebene bereitstellen, da auf diese Weise das bei ZTNA 1.0-Ansätzen vorhandene Problem der „lauten Nachbarn“ vermieden wird.

ZTNA 2.0-Lösungen sollten außerdem mit nativen Digital Experience Monitoring (DEM)-Funktionen ausgestattet sein, die eine proaktive Erkennung von Problemen und ihre automatische Beseitigung unterstützen, um die Anzahl der von IT-Administratoren zu verwaltenden Trouble-Tickets zu reduzieren und so mehr Einblicke und Transparenz zu erhalten, die letztendlich das Benutzererlebnis optimieren.


TECHNISCHES

Laut Gartner ist „Digital Experience Monitoring (DEM) eine Technologie zur Performance-Analyse. DEM unterstützt die Optimierung der operativen Erfahrung und der Interaktionen eines digitalen Agenten – Mensch oder Maschine – mit dem Anwendungs- und Serviceportfolio von Unternehmen . Bei diesen Benutzern, ob menschlich oder digital, kann es sich um eine Kombination aus externen Benutzern handeln, die sich außerhalb und innerhalb der Firewall befinden. Diese Disziplin zielt auch darauf ab, das Verhalten der Nutzer als einen Fluss von Interaktionen in Form einer Customer Journey zu beobachten und zu modellieren.“

Bereitstellung einer einheitlichen Lösung

Bei ZTNA 1.0-Lösungen müssen separate Richtlinien über unterschiedliche Managementkonsolen hinweg verwaltet werden, um alle Benutzer und Anwendungen vollumfänglich zu schützen. Mit ZTNA 1.0 ist es nicht möglich, Vorfälle effektiv zu verhindern bzw. Sicherheitsvorfälle zu erkennen und darauf zu reagieren, da die Verwaltungsfunktionen von Richtlinien und Daten über die gesamte Infrastruktur verteilt sind.

ZTNA 2.0-Lösungen bieten nicht nur überragende Sicherheitsfunktionen, sondern auch eine kompromisslose Performance und eine außergewöhnliche Benutzererfahrung – und das alles auf einer einzigen, einheitlichen Plattform. ZTNA 2.0 stellt eine echte cloud-native Architektur zur Verfügung, die digitale Unternehmen von heute im Cloud-Maßstab sichert und eine kompromisslose Leistung bietet, unterstützt durch Service-Level-Agreements (SLAs) mit Verfügbarkeits- und Performance-Vorgaben. Das resultierende Benutzererlebnis ist in der Tat außergewöhnlich.

Da ZTNA 2.0 vollständig softwarebasiert und hardwareunabhängig ist, kann die Lösung dank automatischer Skalierung mit den sich ändernden hybriden Arbeitsmodellen und Geschäftsanforderungen des Unternehmens automatisch Schritt halten können, ohne Manuelle Prozesse oder Eingriffe sind also nicht nötig.

ERINNERN

ZTNA 2.0-Lösungen stellen ein ganzheitliches Produkt für alle Funktionen dar, einschließlich ZTNA, SWG, Next-Generation CASB, FWaaS, DLP und mehr.

ZTNA UND SASE

In Form von Secure Access Service Edge (SASE) kommen Wide Area Networking (WAN) und Sicherheitsservices in einem einzigen, aus der Cloud bereitgestellten „Service Edge" zusammen, der Unternehmen dabei helfen soll, ihre Netzwerk- und Sicherheitsinfrastrukturen zu modernisieren, um den Anforderungen hybrider Umgebungen und Belegschaften gerecht zu werden.

SASE-Lösungen konsolidieren mehrere Einzelprodukte, darunter ZTNA, Cloud SWG, CASB, FWaaS und Software-Defined Wide-Area Networking (SD-WAN), in einem einzigen integrierten Service, der die Netzwerk- und Sicherheitsinfrastruktur vereinfacht und Unternehmen agiler macht

IN DIESEM KAPITEL

- Abschaffung veralteter Virtual Private Networks
- Schutz von Webanwendungen und Internet-Datenverkehr
- Erweiterter Schutz von SaaS-Anwendungen und Data Loss Prevention

Kapitel 4
Einstieg in ZTNA 2.0

Der Einstieg in Zero Trust Network Access (ZTNA) 2.0 sollte keine übermäßig schwierige oder überwältigende Herausforderung darstellen und auch keine Kompromisse erfordern. Was genau Ihr Unternehmen braucht, hängt von den wichtigsten Belangen und Herausforderungen ab, mit denen Sie aktuell konfrontiert sind. Das Ziel lautet, diese Herausforderungen ohne drastische Eingriffe in Ihre Architektur zu bewältigen. Dieses Kapitel betrachtet drei Anwendungsfälle, die typische Beispiele für einige der größten Herausforderungen darstellen, denen Unternehmen heute gegenüberstehen.

VPN-Ersatz

Remote Access Virtual Private Networks (VPNs) waren jahrelang das Standardtool für die Anbindung von Remote-Benutzern an Unternehmensnetzwerke. Remote Access VPNs tun vor allem eines: Sie ermöglichen Benutzern den sicheren Fernzugriff auf Ressourcen im Unternehmensnetzwerk. Da jedoch immer mehr Anwendungen und Workloads in die Cloud verlagert werden, brauchen Unternehmen heute mehr als Fernzugriff: Sie benötigen auch einen sicheren Zugriff auf Cloud-Anwendungen und das Internet.

Legacy-VPNs verwenden eine Hub-and-Spoke Architektur (siehe Abbildung 4-1), um Remote-Standorte (Spokes) mit einer Zentrale oder einem Rechenzentrum (Hub) zu verbinden. Diese Art

der Verbindung zwischen Standorten ist die optimale Architektur für Rechenzentrumsanwendungen, da das Ziel darin besteht, den „Hub“ zu erreichen, an dem sich die internen Anwendungen und Daten befinden.

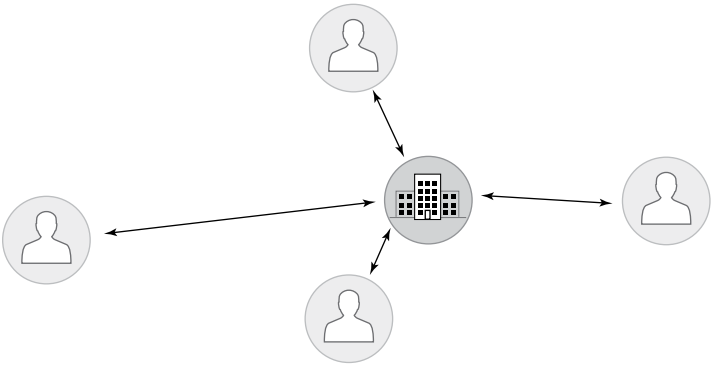

ABBILDUNG 4-1: Hub-and-Spoke-Architektur herkömmlicher VPNs.

Wenn diverse Cloud- und Internet-Anwendungen beteiligt sind, funktioniert dieses Modell jedoch nicht mehr. Bei herkömmlichen VPNs geht der Datenverkehr immer zuerst zum VPN-Konzentrator oder -Gateway, auch wenn die Anwendung in der Cloud gehostet wird (siehe Abbildung 4-2). Der Datenverkehr fließt demzufolge zum VPN-Gateway in der Unternehmenszentrale oder im Rechenzentrum und gelangt dann über die Perimeter-Firewall zum Internet. Die Anwendungsreaktion geht zurück zur Zentrale oder zum Rechenzentrum, bevor sie an den Benutzer weitergeleitet wird. Bei Cloud-Anwendungen folgt dieser Datenverkehr im Wesentlichen einem umständlichen Pfad und unternimmt eine lange (und langsame!) Reise, um einen über das Internet zugänglichen Standort zu erreichen (Tromboning). Vom Sicherheitsstandpunkt aus ist dies sinnvoll, nicht jedoch für die Netzwerkoptimierung.

Tromboning ist ein Verfahren, bei dem der Netzverkehr durch einen Kontrollpunkt (z. B. eine Firewall) geleitet wird. Dabei wird der für das Internet bestimmte Traffic zum Beispiel oft über ein Multiprotocol Label Switching (MPLS)-Netz des Unternehmens und durch eine zentrale Firewall geleitet anstatt über eine direktere Route. Tromboning erhöht die Latenzzeit und die Komplexität des Netzwerks und hat noch weitere negative Auswirkungen.

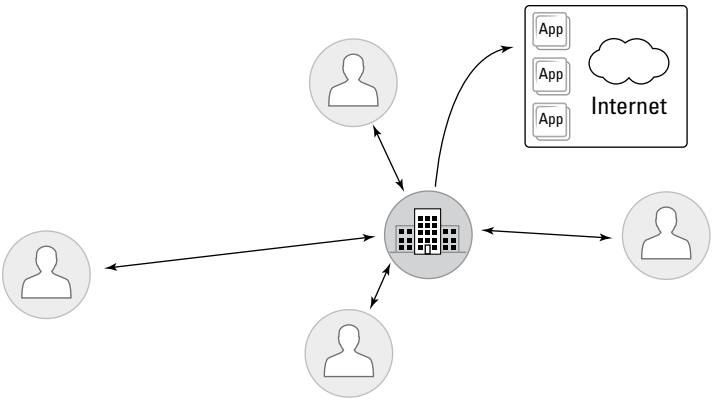

ABBILDUNG 4-2: Herkömmlicher VPNs leiten den Datenverkehr in die Zentrale zurück, bevor er die Cloud erreicht (Backhauling).

Die Verwendung von Cloud-Anwendungen über Legacy-VPNs kann die Benutzererfahrung negativ beeinflussen. Deshalb versuchen viele Endbenutzer, Remote Access VPNs so weit wie möglich zu vermeiden. Sie stellen oft eine Verbindung her, wenn sie Zugriff auf das interne Rechenzentrum benötigen, und brechen die Verbindung wieder ab, wenn kein Zugriff mehr benötigt wird. Dies kann zu einer Reihe von Problemen führen. Wenn Benutzer nicht verbunden sind, verliert das Unternehmen den Überblick über die Anwendungsnutzung, die Kontrolle über den Zugriff auf nicht genehmigte Anwendungen und die Fähigkeit, Sicherheitsrichtlinien durchzusetzen.

Da veraltete VPN-Technologien keine ausreichend granulare Kontrolle ermöglichen und gleichzeitig eine schlechte Performance und unbefriedigende Benutzererfahrung bieten, suchen viele Unternehmen heute nach einer Alternative. Initiativen zum Austausch von VPNs gegen neue Lösungen werden in der Regel durch mehrere Faktoren vorangetrieben, darunter:

- **Anwendungen, die auf ein echtes Hybrid-Modell umgestellt werden und sich On-Premises-, Cloud- und Multi-Cloud-Umgebungen zunutze machen sollen:** Legacy-VPN-Technologien, die den Datenverkehr an einen lokalen „VPN-Konzentrator" weiterleiten, lassen sich nicht skalieren und bieten nicht die bestmögliche Benutzererfahrung.
- **Veränderte Anforderungen an den Zugriff auf Unternehmensanwendungen:** Bisher war in den meisten Unternehmen die Verwendung verwalteter Geräte die Norm, wenn

arbeitsbezogene Aufgaben ausgeführt werden sollten. Inzwischen haben immer mehr nicht verwaltete Geräte wie private Smartphones und Tablets Einzug in Unternehmensnetzwerke gehalten und können auf Unternehmensanwendungen zugreifen.

- **Unternehmen, die nach einem einheitlichen Schutz- und Sicherheitsmodell für alle Anwendungen suchen, nicht nur für Web- oder Legacy-Anwendungen.**

VPN-Technologien wurden nicht zur schnell skalierbaren, hochperformanten und konsistenten Bereitstellung fortschrittlicher Sicherheitsservices entwickelt, um hybriden Belegschaften den sicheren Zugriff auf die von ihnen benötigten Anwendungen zu ermöglichen. Deshalb haben viele Unternehmen damit begonnen, ihre veralteten VPNs durch ZTNA-Lösungen zu ersetzen.

Manche ZTNA-Lösungen können einige dieser Anforderungen erfüllen, doch nur ZTNA 2.0 ist in der Lage, die Netzwerk- und Sicherheitsinfrastruktur derart zu transformieren, dass sowohl verwaltete als auch nicht verwaltete Geräte unterstützt werden und gleichzeitig ein konsistenter Sicherheitsschutz für alle Anwendungen im gesamten Unternehmen zur Verfügung steht.

Wenn Sie Ihr VPN durch eine ZTNA 2.0-Lösung ersetzen, können Sie Zweigstellen, Homeoffices und mobilen Arbeitskräften einen sicheren Fernzugriff auf Anwendungen in der Public und Private Cloud und im Rechenzentrum zur Verfügung stellen (siehe Abbildung 4-3). Zu den wichtigsten Funktionen von ZTNA 2.0 gehören die kontinuierliche Überprüfung des gewährten Vertrauens und kontinuierliche Sicherheitsprüfungen. Dadurch werden die folgenden Ergebnisse erzielt:

- Ein Zero-Trust-Modell für den Zugriff auf private Anwendungen
- Unterstützung für den Zugriff auf verwaltete oder nicht verwaltete Geräte
- Durchgehender Schutz im gesamten Unternehmen

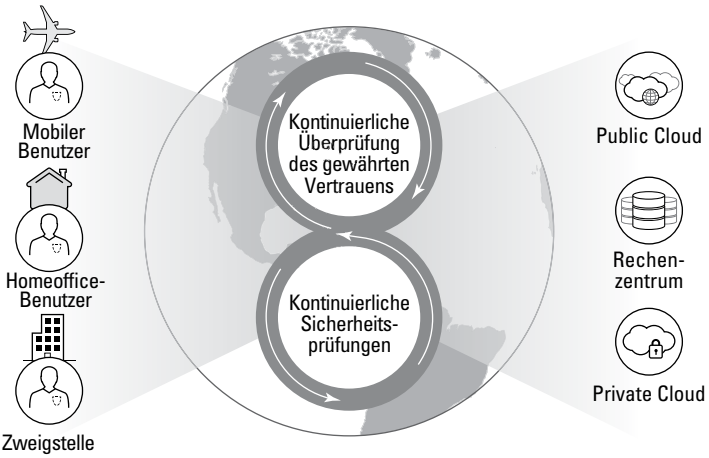

ABBILDUNG 4-3: ZTNA 2.0 als VPN-Ersatz

Die Verwendung von ZTNA 2.0 als VPN-Ersatz bringt unter anderem die folgenden Vorteile mit sich:

- Beste Benutzererfahrung
- Ein einheitliches Produkt
- Integriertes Software-Defined Wide Area Network (SD-WAN)

TIPP

Ersetzen Sie veraltete VPN-Technologien durch eine moderne ZTNA 2.0-Lösung, die einen sicheren Netzwerkzugang für Remote- und Hybrid-Mitarbeiter bietet, Leistungsengpässe überwindet und die Verwaltung vereinfacht.

SICHERER PRIVATER ZUGRIFF FÜR EIN FORTUNE 100-BERATUNGSUNTERNEHMEN

Ein Fortune 100-Beratungsunternehmen wollte sein veraltetes, nicht skalierbares Multi-Vendor-VPN durch eine moderne Fernzugriffslösung ersetzen.

Aufgrund der uneinheitlichen VPN-Lösung hatte das Unternehmen Schwierigkeiten damit, konsistente Transparenz und Sicherheit für seine zahlreichen, über den gesamten Globus verteilten Mitarbeiter und Standorte zu gewährleisten.

(Fortsetzung)

(Fortsetzung)

Außerdem waren die Mitarbeiter des Unternehmens mit dem vorhandenen Sammelsurium an Lösungen unzufrieden. Die Belegschaft hatte regelmäßig mit langsamen Verbindungen, einer von Standort zu Standort unterschiedlichen Performance und einer Benutzererfahrung zu kämpfen, die viel zu wünschen übrig ließ.

Projekttreiber

- Abschaffung einer nicht skalierbaren VPN-Lösung für den Fernzugriff
- Konsistente Transparenz und Sicherheit aller Mitarbeiter, unabhängig von ihrem Aufenthaltsort
- Verbesserung der Benutzererfahrung

Der Kunde benötigte eine moderne Alternative für sein VPN und entschied sich für die Lösung ZTNA 2.0 von Palo Alto Networks. Mit ZTNA 2.0 ist das Unternehmen nun in der Lage, konsistente Verbindungen für alle 350.000 Benutzer in 158 Ländern und einen direkten sicheren Internetzugang für Hunderte von Zweigstellen auf der ganzen Welt bereitzustellen. Darüber hinaus gewährleistet ZTNA 2.0 einen konsistenten und sicheren Zugriff auf alle Anwendungen, einschließlich Legacy-Anwendungen, über mehr als 30 Rechenzentren und Cloud-Standorte hinweg.

Auswirkungen

- Schutz von 350.000 Benutzern in 158 Ländern
- Lokales Internet mit Sicherheitsfunktionen aus der Cloud zum Schutz von Hunderten von Büros auf der ganzen Welt
- ZTNA für Tausende von Anwendungen in mehr als 30 Rechenzentren und Cloud-Standorten

Sicherer Internetzugang

Unternehmen nutzen viele Anwendungen. Einige davon befinden sich vor Ort, andere in der Cloud. Durch die Zunahme mobiler und hybrider Belegschaften wird es immer schwieriger, Remote-Benutzer vor Bedrohungen zu schützen, wenn sie auf diese Anwendungen zugreifen wollen.

Der Zugriff auf lokale Anwendungen erfolgt in der Regel über ein Remote Access VPN. Wenn Benutzer auf internetbasierte Anwendungen und Services zugreifen wollen, muss ihre Verbindung zu diesem

VPN jedoch abgebrochen werden. Dadurch entstehen Sicherheitsrisiken. Unternehmen verwenden Secure Web Gateways (SWGs), um Remote-Benutzern, die nicht mit dem VPN verbunden sind, einen sicheren Internetzugang zur Verfügung zu stellen.

Ein SWG fungiert gewöhnlich als ein *Proxy* (Vermittler) zwischen Benutzern und Internetressourcen, um Benutzer vor Bedrohungen aus dem Internet zu schützen und die Unternehmensrichtlinien zur akzeptablen Nutzung anzuwenden und durchzusetzen. Anstatt sich direkt mit einer Website zu verbinden, wird der Benutzer an das SWG weitergeleitet, das dann dafür verantwortlich ist, ihn mit der gewünschten Website zu verbinden und Funktionen wie Uniform Resource Locator (URL)-Filterung, Web-Transparenz, Malware-Prüfung, Web-Zugangskontrollen und andere Sicherheitsmaßnahmen auszuführen.

ERINNERN

Mit einem SWG können Unternehmen

- den Zugang zu unangemessenen Websites oder Inhalten auf der Grundlage von Richtlinien zur akzeptablen Nutzung sperren,
- Sicherheitsrichtlinien durchsetzen, um den Internetzugang sicherer zu machen,
- Daten vor der unbefugten Übertragung schützen.

Allerdings werden herkömmliche SWGs in der Regel als Appliances in Unternehmensnetzwerken eingesetzt, sodass der Benutzerdatenverkehr zu den SWGs umgeleitet werden muss, die sich häufig in einem Unternehmensrechenzentrum befinden. Dieses ineffiziente Routing des Datenverkehrs erhöht die Latenzzeit und wirkt sich negativ auf die Benutzerfreundlichkeit aus.

Eine weitere Herausforderung besteht darin, dass es sich bei älteren SWGs in der Regel um eigenständige Lösungen handelt, die nicht in der Lage sind, Workflows, Berichte oder Protokolle mit anderen Sicherheitsinfrastrukturen im Unternehmen zu koordinieren. Die Komplexität kann sich mit der Zeit erhöhen, da Unternehmen oft mehrere Sicherheitsprodukte einsetzen, die ihre Sicherheitsabläufe in puncto Effizienz und Effektivität beeinträchtigen.

Für Unternehmen, die die Benutzererfahrung ihrer Mitarbeiter beim Zugriff auf das Internet und auf Webanwendungen verbessern möchten, stellen die cloudbasierten SWG-Funktionen von ZTNA 2.0 eine effektive Lösung dar, da Latenzzeiten verkürzt werden und ein höheres Sicherheitsniveau erreicht wird (siehe Abbildung 4-4).

ABB. 4-4: ZTNA 2.0 als SWG-Ersatz/Cloud SWG.

TIPP

Bei der Bewertung von ZTNA 2.0 als Alternative für ältere SWG-Produkte sollten die folgenden Anforderungen berücksichtigt werden:

- **Erfordert keine wesentlichen Änderungen am Netzwerk:** Viele Unternehmen möchten ihre bestehenden proxybasierten Lösungen beibehalten, um Unterbrechungen auf ein Minimum zu begrenzen und eine Neuaufstellung des Netzwerks zu vermeiden.
- **Bietet die Möglichkeit eines agentenbasierten Ansatzes:** Die Option, Agenten auf den Endgeräten von Benutzern zu installieren, ist wünschenswert, sollte aber nicht das einzige verfügbare Bereitstellungsmodell sein.
- **Ermöglicht die konsistente Durchsetzung von Richtlinien:** Die Lösung muss eine konsistente Durchsetzung von Richtlinien für die hybride Belegschaft des Unternehmens bieten, die mobile, Homeoffice- und Zweigstellenbenutzer umfasst.

SICHERER INTERNETZUGANG FÜR EIN FORTUNE 100-PHARMAUNTERNEHMEN

Ein Fortune 100-Pharmaunternehmen wollte seine von mehreren Herstellern bereitgestellte On-Premises-Hardware reduzieren und

seine Infrastruktur mit cloudbasierten Sicherheitsfunktionen modernisieren.

Da immer mehr der von Mitarbeitern benötigten Tools und Anwendungen in die Cloud verlagert wurden, konnten die vorhandenen Lösungen den Benutzern nicht die erwartete nahtlose Erfahrung bieten, womit diese naturgemäß unzufrieden waren.

Der Kunde benötigte einen modernen, cloudbasierten Sicherheitsansatz und entschied sich für die ZTNA 2.0-Lösung von Palo Alto Networks. Dank der Proxy-Fähigkeit von ZTNA 2.0 war das Unternehmen in der Lage, alle 100.000 Benutzer innerhalb von drei Monaten zu migrieren, ohne sein Netzwerk umgestalten zu müssen.

Die neue, cloudnative Lösung konsolidierte bzw. eliminierte die Proxy-Hardware vor Ort und ermöglichte es dem Unternehmen, das Sicherheitsniveau für alle Benutzer und Standorte zu verbessern. Darüber hinaus wurden die nativen Autonomous Digital Experience Management (ADEM)-Funktionen von Prisma Access eingesetzt, um eine außergewöhnliche Benutzererfahrung für alle Hybrid-Mitarbeiter zu gewährleisten.

Projekttreiber

- Migration in die Cloud
- Reduzierung der On-Premises-Hardware
- Verbesserte Benutzererfahrung

Auswirkungen

- 100.000 Benutzer in weniger als drei Monaten migriert
- On-Premises SWG-Hardware durch cloudnative Lösung ersetzt
- Erhebliche Verbesserung des Sicherheitsniveaus
- Außergewöhnliche Benutzererfahrung mit ADEM

Erweiterte SaaS-Sicherheit

Früher befanden sich die Anwendungen und Daten von Unternehmen gewöhnlich in einem On-Premises-Rechenzentrum. Diese Umgebung bot Unternehmen umfassende Transparenz und granulare Kontrolle. Sie wussten jederzeit, wer wann auf ihre Anwendungen und Daten zugriff und welche Geräte (in der Regel Desktop- oder Laptop-Computer) dabei verwendet wurden.

Unternehmen, die damit begannen, ihre Daten in die Cloud zu verlagern und Cloud-Services wie SaaS-Anwendungen zu nutzen, wussten plötzlich nicht mehr, wer auf ihre Cloud-Anwendungen und -Daten Zugriff hatte und diese nutzte oder – dank der Einführung mobiler Technologien wie Laptops und Smartphones – mit welchen Geräten diese Cloud-Services verwendet wurden. Die Verbreitung und Benutzerfreundlichkeit von SaaS-Anwendungen führte außerdem häufig zur Entstehung einer „Schatten-IT", d. h., Benutzer verwendeten nicht genehmigte oder zugelassene Anwendungen für geschäftliche Zwecke und gefährdeten dadurch unbeabsichtigt die sensiblen Daten des Unternehmens.

Diese mangelnde Transparenz führt zu einem unzureichenden Schutz der Daten und macht Unternehmen anfällig für eine Vielzahl von Sicherheitsrisiken, z. B. Datenpannen, Nichteinhaltung gesetzlicher Vorschriften, Malware oder Ransomware.

Zur Bewältigung dieser Herausforderungen entwickelten Sicherheitsanbieter Cloud Access Security Broker (CASB)-Lösungen. Mithilfe von CASBs können Unternehmen herausfinden, wo sich ihre Daten in SaaS-Anwendungen befinden und wann sie übertragen werden, z. B. in Cloud-Service-Umgebungen, On-Premises-Rechenzentren oder von mobilen Mitarbeitern. Ein CASB setzt auch die Sicherheits-, Governance- und Compliance-Richtlinien des Unternehmens um. Er kontrolliert den Zugriff auf Cloud-Anwendungen und hilft Unternehmen dabei, ihre sensiblen Daten effektiv und konsistent über mehrere Standorte hinweg zu schützen.

Allerdings sind herkömmliche CASB-Lösungen nicht in der Lage, neue Cloud-Anwendungen schnell einzubinden, da sie auf statischen Anwendungsbibliotheken basieren, die manuell mit Daten befüllt werden müssen. Moderne Collaboration-Apps wie Slack, Zoom, Confluence oder Jira, mit denen Benutzer heute die meiste Zeit verbringen, werden in der Regel nicht von den API-Schutzfunktionen dieser CASB-Lösungen abgedeckt.

Eine herkömmliche CASB-Lösung verfügt über grundlegende Cloud-Sicherheitsfunktionen, die in der Breite und Tiefe begrenzt sind und daher nur eine punktuelle Sicherheit bieten. Ihre Data Loss Prevention (DLP)-Funktionen sind zum Beispiel relativ elementar und ungenau und decken nur Daten in bestimmten SaaS-Anwendungen ab. Gleichzeitig sind sie völlig von den DLP-Funktionen losgelöst, die den Rest des Unternehmens schützen. Außerdem fehlen wesentliche Mechanismen zur Bedrohungsabwehr, die die zahlreichen

Bedrohungsvarianten erkennen können, die Cyberkriminelle für Angriffe auf SaaS-Anwendungen nutzen.

CASB-Lösungen wurden ursprünglich als eigenständige, proxybasierte Punktlösungen konzipiert. Das Problem bei proxybasierten CASBs besteht darin, dass sie eine komplexe Umleitung des Datenverkehrs von der Netzwerk-Firewall mit Proxy Auto-Configuration (PAC)-Agenten und Protokollsammlern erfordern. Dies erhöht die Komplexität von IT-Prozessen und -Architekturen und führt zu hohen Betriebskosten.

Viele Unternehmen, die Legacy-CASB-Lösungen einsetzen, können mit der schnellen Zunahme von SaaS-Anwendungen und Schatten-IT, dem allgegenwärtigen Datenwachstum und der zunehmenden Zahl von Hybrid- und Remote-Mitarbeitern nicht mehr Schritt halten. Unternehmen, die Legacy-CASBs durch CASBs der nächsten Generation im Rahmen einer Secure Access Service Edge (SASE)-Architektur mit ZTNA 2.0 ersetzen, können Cloud-Services mit kontinuierlichen Vertrauens- und Sicherheitsüberprüfungen nutzen. Dies umfasst die folgenden Funktionen (siehe Abbildung 4-5):

- Transparenz und Kontrolle über SaaS-Anwendungen
- Schutz von genehmigten SaaS-Anwendungen
- Erweiterte DLP-Funktionen

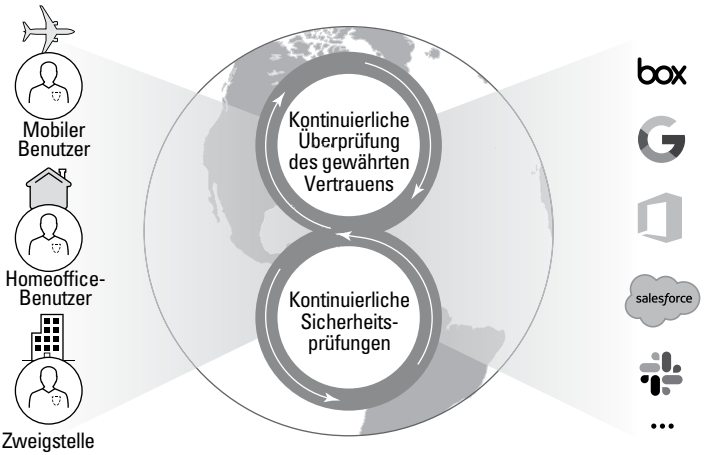

ABBILDUNG 4-5: ZTNA 2.0 für erweitere Sicherheit von SaaS-Anwendungen/CASBs der nächsten Generation.

ERWEITERTE SICHERHEIT FÜR DIE SAAS-ANWENDUNGEN EINES GROSSEN AUTOMOBILZULIEFERERS

Ein weltweit führendes Automotive-Unternehmen mit mehr als 190.000 Mitarbeitern und Hunderten von Produktionsstätten, zahlreichen technischen Zentren auf der ganzen Welt und einer Präsenz in mehr als 40 Ländern nutzte immer mehr Anwendungen in der Cloud. Das Unternehmen benötigte mehr Transparenz und granulare Kontrolle über bekannte und unbekannte SaaS-Anwendungen, eine konsolidierte Verwaltung von Produkten mehrerer Anbieter und eine integrierte Bedrohungserkennung.

Das Unternehmen suchte auch nach einer Lösung zur einfachen Richtlinienerstellung und -implementierung ohne Proxy oder Agenten und wollte Risiken, Richtlinien und Ziele nicht mehr auf einer separaten Schicht des Stacks synchronisieren.

Mit der ZTNA 2.0-Lösung von Palo Alto Networks mit -CASB-Funktionen der nächsten Generation war es nicht mehr erforderlich, Agenten zur Inline-Inspektion und zum Schutz nicht verwalteter Endpunkte zu aktualisieren und zu konfigurieren.

Projekttreiber

- Umfassende Cloud-/SaaS-Einführung
- Transparenz und Kontrolle über bekannte und unbekannte Anwendungen
- Weniger Komplexität, konsolidierte Sicherheit

Auswirkungen

- Vereinfachte Bereitstellung und Richtlinienerstellung durch cloudbasierte Sicherheit
- Deutlich verbesserte Transparenz und Kontrolle über alle Anwendungen
- Konsistenter Schutz für 190.000 Benutzer weltweit

IN DIESEM KAPITEL

- Vollständige Transparenz und Kontrolle
- Kontinuierliche Überprüfung des gewährten Vertrauens
- Schutz aller Anwendungen durch eine einheitliche Lösung
- Umfassende Sicherheitsprüfung
- Verhinderung von Datenverlusten in allen Umgebungen
- Gewährleistung der Anwendungsverfügbarkeit und -Performance
- Reduzierung von Komplexität und Kosten durch eine einzige Lösung

Kapitel 5
Fragen, die Sie dem Anbieter Ihrer ZTNA 2.0-Lösung stellen sollten

Die folgenden wichtigen Fragen sollen Ihnen dabei helfen, potenzielle Anbieter von Zero Trust Network Access (ZTNA) 2.0-Lösungen zu bewerten.

Bietet die Lösung vollständige Layer-7-Anwendungstransparenz?

Benutzer verwenden immer häufiger eine Vielzahl von Anwendungen für arbeitsbezogene sowie persönliche Zwecke von mehreren Geräten und Standorten aus, darunter auch unterschiedliche SaaS-Anwendungen. Viele Anwendungen, wie Instant Messaging (IM), Peer-to-Peer-Dateifreigabe (P2P) und Voice over Internet Protocol (VoIP) können auf nicht standardmäßigen oder dynamischen Ports und IP-Adressen betrieben werden.

Darüber hinaus werden viele Benutzer immer versierter darin, Anwendungen durch Protokolle wie Remote Desktop Protocol (RDP) und Secure Shell (SSH) dazu zu zwingen, über nicht standardmäßige Ports zu laufen. Die Richtlinien des Unternehmens bezüglich verschiedener Anwendungen (genehmigt, toleriert, nicht genehmigt) werden dabei gern außer Acht gelassen. Eine ZTNA-Lösung, die Anwendungen auf der Grundlage willkürlicher Layer-3-Portzuweisungen identifiziert und auf Layer-3- oder Layer-4-Zugriffskontrolle beschränkt ist, reicht für den Schutz Ihres Unternehmens nicht mehr aus.


TIPP

Halten Sie nach einer ZTNA 2.0-Lösung Ausschau, die den Datenverkehr standardmäßig jederzeit auf allen Ports nach Anwendung klassifizieren kann und dabei keinen Verwaltungsaufwand verursacht. Sie sollten nicht nachforschen müssen, welche Anwendungen welche Ports verwenden, um geeignete Richtlinien und Regeln zu konfigurieren. Eine umfassende ZTNA 2.0-Lösung bietet umfassende Transparenz über die Nutzung von Anwendungen auf Layer 7 (Application) sowie Transparenz und Kontrolle darüber.

Bietet die Lösung eine kontinuierliche Überprüfung des gewährten Vertrauens?

Das Grundprinzip von Zero Trust lautet „Niemals vertrauen, immer überprüfen“ – nicht „Niemals vertrauen, einmal überprüfen“ oder „Niemals vertrauen, gelegentlich überprüfen“. Einem Akteur auf der Grundlage statischer Anmeldedaten zu vertrauen, die nur einmal auf einem Gerät überprüft wurden, das zu einem bestimmten Zeitpunkt vertrauenswürdig erschien, ist der sicherste Weg in die Katastrophe. Cyberkriminelle nutzen dieses fragwürdige Vertrauensmodell, um sich frei in einer Netzwerkumgebung zu bewegen, nachdem sie die Schutzeinrichtungen am Perimeter durchbrochen haben.


TIPP

Eine zuverlässige ZTNA 2.0-Lösung führt kontinuierliche Vertrauensüberprüfungen auf der Grundlage des Verhaltens einzelner Benutzer durch und verwendet maschinelles Lernen (ML), um Risiken einzuschätzen und potenzielle Bedrohungen zu erkennen. Der Zugriff auf das Netzwerk oder auf eine Anwendung sollte nur nach einer sorgfältigen Überprüfung von Benutzern und Geräten gestattet werden, die Multifaktor-Authentifizierung (MFA) umfasst. Doch das ist noch nicht alles. Die fortlaufende Vertrauensüberprüfung sollte kontinuierlich und nahtlos während der gesamten Sitzung stattfinden, um sicherzustellen, dass sich der Sicherheitsstatus des Benutzers oder Geräts nicht geändert hat oder kompromittiert worden ist.

Schützt die Lösung alle Anwendungen konsistent mit einem einzigen Produkt?

Wie in Kapitel 1 erklärt wird, führen punktuelle Sicherheitslösungen, die nur bestimmte Anwendungen schützen oder begrenzte Anwendungsszenarien unterstützen, zu Komplexität, Ineffizienz und letztlich zu einem schwächeren Sicherheitsstatus. Sie müssen damit rechnen, dass Benutzer kreative neue Wege finden werden, um verwirrende und umständliche Sicherheitskontrollen zu umgehen. Sicherheitsteams machen eher Fehler, wenn sie Tools mit unterschiedlichen Betriebssystemen, Schnittstellen und Syntaxen konfigurieren und verwenden müssen. Gleichzeitig werden sie mit Warnmeldungen überflutet, die nicht einfach mit spezifischen Bedrohungen in einer integrierten Lösung in Verbindung gebracht werden können.

TIPP

Ihre ZTNA 2.0-Lösung sollte in der Lage sein, alle Ihre Anwendungen mit einem einzigen, einheitlichen Produkt konsistent zu sichern, einschließlich älterer benutzerdefinierter Anwendungen, moderner cloudnativer Anwendungen auf Microservices-Basis sowie SaaS-Anwendungen.

Führt die Lösung umfassende Sicherheitsprüfungen durch?

Eine ZTNA 2.0 Lösung muss mehr tun, als den Datenverkehr auf der Grundlage einer eingeschränkten Prüfung von Paket-Headern und der Durchsetzung statischer Firewall-Regeln zuzulassen oder zu sperren. Sie muss auch fortschrittliche Malware, einschließlich Ransomware, abwehren und sowohl bekannte als auch unbekannte Bedrohungen im verschlüsselten und unverschlüsselten Anwendungs-Traffic und Datenverkehr aufspüren können – und zwar im gesamten Anwendungs-Traffic, nicht nur in privaten Anwendungen.

TIPP

Eine umfassende ZTNA 2.0-Lösung muss vollständige Sicherheitsüberprüfungen und -kontrollen bieten, einschließlich Malware- und Bedrohungsabwehr.

Bietet die Lösung einen konsistenten Schutz für alle Unternehmensdaten?

Ein konsistenter Schutz aller Daten erfordert die Konsolidierung von Datenschutzrichtlinien für alle Umgebungen und Datenübertragungsvektoren. Unzusammenhängende Datenschutzrichtlinien

und -konfigurationen für unterschiedliche SaaS-Anwendungen, On-Premises-Repositorys, E-Mail-Kommunikation, lokale Speicher usw. führen zu blinden Flecken, komplexen Verwaltungsabläufen, inkonsistenten Kontrollen und Schatten-IT.


TIPP

Wählen Sie eine ZTNA 2.0-Lösung, die die Verwendung einer einheitlichen Data Loss Prevention (DLP)-Schutzrichtlinie in jeder Umgebung ermöglicht, in der sich Daten befinden.

Werden SLAs mit Verfügbarkeits- und Performance-Vorgaben für alle Anwendungen zur Verfügung gestellt?

Sicherheitstools, die sich negativ auf die Verfügbarkeit und Performance von Anwendungen auswirken, tragen zu einer schlechten Benutzererfahrung bei, die letztlich zu mehr Schatten-IT führt: Benutzer suchen nach neuen Möglichkeiten, die Sicherheitstools zu umgehen, die sie eigentlich schützen sollen.


TIPP

Moderne ZTNA 2.0-Lösungen werden in der Cloud bereitgestellt und müssen daher Zuverlässigkeits- und Leistungsgarantien bieten, damit Benutzer die benötigten Anwendungen – auch interne und SaaS-basierte – sicher und effizient nutzen können. Stellen Sie sicher, dass Ihr ZTNA 2.0-Anbieter Service Level Agreements (SLAs) für die Verfügbarkeit und Performance anbietet, die den Anforderungen Ihres Unternehmens entsprechen.

Haben Sie ein einziges, einheitliches Produkt zum Schutz des Unternehmens?

Isolierte Sicherheitstools, die sich nicht problemlos in andere Lösungen integrieren lassen, verursachen zusätzliche Kosten und Komplexität in Ihrer Umgebung und können die Erkennung, Korrelation, Identifizierung von kritischen Bedrohungen sowie die Reaktion darauf verzögern. Diese zusätzliche Komplexität führt letztendlich zu einem höheren Verwaltungsaufwand und erhöht gleichzeitig die Risiken und die Gefährdungslage des Unternehmens.


TIPP

Ein ZTNA 2.0-Anbieter sollte eine einzige, einheitliche Lösung anbieten, z. B. Secure Access Service Edge (SASE), die Ihr gesamtes Unternehmen schützt – Benutzer, Anwendungen, Geräte und Daten, unabhängig von deren Stand- bzw. Speicherort –, um Risiken zu verringern und bessere Sicherheitsergebnisse zu erzielen.

Glossar

ADEM: *Siehe* Autonomous Digital Experience Management (ADEM).

AI: *Siehe* Künstliche Intelligenz (KI).

Antivirus (AV): Software, die Computerviren und andere Malware erkennt und verhindert, dass sie Systeme infizieren. *Siehe auch* Malware.

API: *Siehe* Application Programming Interface (API).

Application Programming Interface (API): Eine Suite von Protokollen, Routinen und Tools, die zur Entwicklung und Integration von Anwendungen verwendet werden.

Künstliche Intelligenz (KI): Die Fähigkeit eines Computers, mit seiner Umgebung zu interagieren, aus ihr zu lernen und automatisch Aktionen auszuführen, ohne speziell dafür programmiert worden zu sein.

Autonomous Digital Experience Management (ADEM): Eine Funktion von Palo Alto Networks Prisma Access, die eine SASE-native Überwachung der digitalen Erfahrung sowie vollständige Transparenz bietet und dafür sorgt, dass Netzwerkprobleme automatisch behoben werden, bevor oder während sie auftreten. *Siehe auch* Secure Access Service Edge (SASE).

AV: *Siehe* Antivirus (AV).

C2: *Siehe* Command-and-Control (C2).

Command-and-Control (C2): Kommunikationsverbindungen zwischen Malware und/oder kompromittierten Systemen einerseits und der Remote-serverinfrastruktur eines Angreifers andererseits, über die bösartige Befehle gesendet bzw. empfangen oder Daten ausgeschleust werden.

Data Loss Prevention (DLP): Eine Anwendung oder ein Gerät zur Erkennung der unbefugten Speicherung oder Übertragung sensibler Daten.

Deep Packet Inspection (DPI): Eine fortschrittliche Methode zur Untersuchung und Verwaltung des Netzdatenverkehrs, bei der nicht nur die ursprünglichen Paket-Header überprüft werden.

DLP: *Siehe* Data Loss Prevention (DLP).

DNS: *Siehe* Domain Name System (DNS).

Domain Name System (DNS): Eine hierarchische, dezentralisierte Verzeichnisdienst-Datenbank, die Domainnamen und die IP-Adressen der dazugehörigen Computer, Services und anderen mit einem Netzwerk oder dem Internet verbundenen IT-Ressourcen enthält und ineinander umwandelt. *Siehe auch* Internet Protocol (IP).

DPI: *Siehe* Deep Packet Inspection (DPI).

EDR: *Siehe* Endpoint Detection and Response (EDR).

Endpoint Detection and Response (EDR): Eine Kategorie von Tools zur Erkennung und Untersuchung von Bedrohungen auf Endpunkten. EDR-Tools bieten in der Regel Funktionen zur Erkennung, Untersuchung, Suche nach und Reaktion auf Bedrohungen.

Endpoint Protection Platform (EPP): Eine integrierte Sicherheitssuite, die Technologien zum Schutz von Endgeräten umfasst, darunter Antivirustools, Datenverschlüsselung, Data Loss Prevention, eine Personal Firewall sowie Port- und Gerätekontrolle.

EPP: *Siehe* Endpoint Protection Platform (EPP).

Exploit: Software oder Code, die/der eine Schwachstelle in einem Betriebssystem oder einer Anwendung ausnutzt und unerwünschtes Verhalten im Betriebssystem oder in der Anwendung verursacht, z. B. Rechteausweitung, Fernsteuerung oder einen Denial-of-Service-Angriff.

Firewall-as-a-Service (FWaaS): Eine Firewall-Plattform, die als Service in einer Cloud-Umgebung angeboten wird.

FWaaS: *Siehe* Firewall-as-a-Service (FWaaS).

Hybrid-Cloud: Eine Umgebung, die Ressourcen mehrerer Public und/oder Private Clouds miteinander verbindet und die Verlagerung von Anwendungen und Daten zwischen diesen Clouds ermöglicht. *Siehe auch* Private Cloud *und* Public Cloud.

IM: *Siehe* Instant Messaging (IM).

Instant Messaging (IM): Eine Variante von Echtzeit-Online-Chats über das Internet.

Internet Protocol (IP): Das Protokoll für Layer 3 des OSI-Modells, das die Grundlage des modernen Internets bildet. *Siehe auch* Open Systems Interconnection-Modell (OSI).

Intrusion Prevention System (IPS): Eine Hardware- oder Softwareanwendung, die mutmaßliche Netzwerk- oder Host-Eindringversuche erkennt und abwehrt.

IP: *Siehe* Internet Protocol (IP).

IPS: *Siehe* Intrusion Prevention System (IPS).

LAN: *Siehe* Local Area Network (LAN).

Local Area Network (LAN): Ein Netzwerk, das Computer in einem relativ kleinen Bereich miteinander verbindet, z. B. einem Bürogebäude, Lager oder Wohnhaus.

Maschinelles Lernen (ML): Eine Methode der Datenanalyse, mit der Computer einen Datensatz analysieren und aufgrund der Ergebnisse automatisch Aktionen durchführen können, ohne speziell dafür programmiert worden zu sein.

Malware: Schadsoftware oder bösartiger Code, die/der in der Regel Computersysteme schädigt oder deaktiviert, die Kontrolle über sie übernimmt oder Daten von ihnen stiehlt.

MFA: *Siehe* Multifaktor-Authentifizierung (MFA).

ML: *Siehe* Maschinelles Lernen (ML).

MPLS: *Siehe* Multiprotocol Label Switching (MPLS).

Multi-Cloud: Eine Umgebung, die Ressourcen mehrerer Public und/oder Private Clouds miteinander verbindet, aber nicht unbedingt die Verlagerung von Anwendungen und Daten zwischen diesen Clouds unterstützt (d. h., die unterschiedlichen Cloud-Umgebungen können als isolierte Clouds betrieben werden). Wichtiger Hinweis: Alle Hybrid-Cloud-Umgebungen sind auch Multi-Cloud-Umgebungen, doch nicht jede Multi-Cloud-Umgebung ist eine Hybrid-Cloud-Umgebung. *Siehe auch* Hybrid Cloud, Private Cloud *und* Public Cloud.

Multifaktor-Authentifizierung (MFA): Ein Authentifizierungsmechanismus, der zwei oder mehrere der folgenden Faktoren erfordert: etwas, das der Anwender kennt; etwas, das der Anwender besitzt oder etwas, das der Anwender ist. Ein Benutzer kann sich beispielsweise mit seinem Benutzernamen und seinem Passwort authentifizieren (die er kennt) und dann auf einem zuvor bei seinem Unternehmen registrierten Mobiltelefon (das er besitzt) einen einmaligen Passcode empfangen.

Multiprotocol Label Switching (MPLS): Ein Verfahren zur Weiterleitung von Paketen durch ein Netzwerk unter Verwendung von Labels, die zwischen den Layer-2- und Layer-3-Headern der Datenpakete eingefügt werden.

Network Traffic Analysis (NTA): Eine Kategorie von Tools zum Abfangen, Aufzeichnen und Analysieren von Mustern im Netzwerkdatenverkehr, um mithilfe einer Kombination aus maschinellem Lernen, Verhaltensmodellierung und regelbasierter Erkennung Anomalien und verdächtige Aktivitäten zu erkennen und darauf zu reagieren. *Siehe auch* Maschinelles Lernen.

NTA: *Siehe* Network Traffic Analysis (NTA).

Open Systems Interconnection-Modell (OSI): Das aus sieben Schichten bestehende Referenzmodell für Netzwerke. Diese Schichten sind: Bitübertragungsschicht (Physical Layer), Sicherungsschicht (Data Link Layer), Vermittlungsschicht (Network Layer), Transportschicht (Transport Layer), Sitzungsschicht (Session Layer), Darstellungsschicht (Presentation Layer) und Anwendungsschicht (Application Layer).

OSI-Modell: *Siehe* Open Systems Interconnection-Modell (OSI-Modell).

P2P: *Siehe* Peer-to-Peer (P2P).

PAC: *Siehe* Proxy-Autokonfigurationsdatei (PAC-Datei).

Peer-to-Peer (P2P): Eine verteilte Anwendungsarchitektur, die Freigaben zwischen Knoten ermöglicht.

Proxy-Autokonfigurationsdatei (PAC-Datei): Ein webbasierter, in JavaScript geschriebener Regelsatz, der Ihren Endpunkten Anweisungen zum Routen von Datenverkehr für bestimmte URLs gibt: entweder über einen Web-Proxy oder direkt zum Internet. Eine PAC-Datei kann Informationen wie die IP-Adresse der Website, die IP-Adresse des Benutzers und den Namen des Hosts enthalten, der die Website angefordert hat. *Siehe* auch Uniform Resource Locator (URL).

Private Cloud: Ein Cloud-Computing-Bereitstellungsmodell, das aus einer Cloud-Infrastruktur besteht, die ausschließlich von einer einzigen Organisation genutzt wird.

Public Cloud: Ein Cloud-Computing-Bereitstellungsmodell, das aus einer Cloud-Infrastruktur besteht, die von der allgemeinen Öffentlichkeit genutzt werden kann.

RDP: *Siehe* Remote Desktop Protocol (RDP).

Remote Desktop Protocol (RDP): Ein proprietäres Microsoft-Protokoll, das den Remotezugriff auf einen Computer ermöglicht. RDP verwendet standardmäßig TCP-Port 3389 und UDP-Port 3389. *Siehe auch* Transmission Control Protocol (TCP) *und* User Datagram Protocol (UDP).

SaaS: *Siehe* Software-as-a-Service (SaaS).

SDP: *Siehe* Software-Defined Perimeter (SDP).

SD-WAN: *Siehe* Software-Defined Wide Area Network (SD-WAN).

Secure Shell (SSH): Ein kryptografisches Netzwerkprotokoll, das sicheren Zugang zu einem entfernten Computer bietet.

Secure Web Gateway (SWG): Eine Sicherheitsplattform oder ein Sicherheitsservice, die/der alle Arten von Traffic überwacht und Umgehungsversuche enttarnt, hinter denen sich Bedrohungen verbergen können. Secure Web Gateways können über zusätzliche Funktionen verfügen, darunter die Filterung von Webinhalten und die Verhinderung von Identitätsdiebstahl.

Security Information and Event Management (SIEM): Ein System zur Erfassung, Analyse, Korrelation und Darstellung von Sicherheitsprotokollen und Warnmeldungen in Echtzeit. Die Analysten in Security Operations Centern (SOC) verwenden SIEM-Tools zur Verwaltung von Sicherheitsvorfällen und zur schnellen Erkennung von und Reaktion auf potenzielle Bedrohungen. *Siehe auch* Security Operations Center (SOC).

Security Operations Center (SOC): Eine Abteilung, die für die Überwachung der Cybersicherheit, die Bewertung und Abwehr von Bedrohungen und die Behebung von Sicherheitsvorfällen zum Schutz der Computer- und Netzwerkressourcen von Unternehmen verantwortlich ist, einschließlich On-Premises- und Cloud-Umgebungen.

Service-Level Agreement (SLA): Formale Mindestleistungsstandards für Systeme, Anwendungen, Netzwerke oder Services.

Schatten-IT: IT-Anwendungen und -Services, die von Endbenutzern ohne ausdrückliche Genehmigung des Unternehmens und oft ohne Kenntnis oder Unterstützung der IT-Abteilung erworben und benutzt werden.

SIEM: *Siehe* Security Information and Event Management (SIEM).

SLA: Siehe Service-Level Agreement (SLA).

SOC: *Siehe* Security Operations Center (SOC).

Software-as-a-Service (SaaS): Ein cloudbasiertes Software-Vertriebsmodell, bei dem ein Drittanbieter Anwendungen hostet, die er Kunden über das Internet zur Verfügung stellt. Der Softwareanbieter hostet und verwaltet die Server, die Datenbanken und den Code der Anwendung.

Software-Defined Perimeter (SDP): Ein softwaredefinierter Perimeter sichert sämtliche Verbindungen zu den Services auf allen Ebenen einer Netzwerkinfrastruktur ab, wobei das Sicherheitsniveau vom Benutzer definiert und etabliert wird.

Software-Defined Wide Area Network (SD-WAN): Ein neuer Ansatz für Weitverkehrsnetze, bei dem die Prozesse der Netzwerksteuerung und -verwaltung von der zugrunde liegenden Hardware getrennt und als Software verfügbar gemacht werden. *Siehe auch* Wide Area Network (WAN).

SSH: *Siehe* Secure Shell (SSH).

SWG: *Siehe* Secure Web Gateway (SWG).

Taktiken, Techniken und Verfahren (TTPs): Die Verhaltensweisen, Methoden, Strategien und Tools, die von Bedrohungsakteuren zum Angriff auf ein Ziel verwendet werden.

TCP: *Siehe* Transmission Control Protocol (TCP).

Transmission Control Protocol (TCP): Ein verbindungsorientiertes Protokoll, das für die Herstellung einer Verbindung zwischen zwei Hosts verantwortlich ist und die Übermittlung von Daten und Paketen in der richtigen Reihenfolge garantiert.

Tromboning: Ein Verfahren, bei dem der Netzwerkdatenverkehr durch einen Kontrollpunkt (z. B. eine Firewall) geleitet wird.

TTPs: *Siehe* Taktiken, Techniken und Verfahren (TTPs).

UDP: *Siehe* User Datagram Protocol (UDP).

UEBA: *Siehe* User and Entity Behavior Analytics (UEBA).

Uniform Resource Locator (URL): Gemeinhin als „Webadresse" oder „Internetadresse" bekannt. Ein eindeutiger Identifikator einer mit dem Internet verbundenen Ressource.

URL: *Siehe* Uniform Resource Locator (URL).

User and Entity Behavior Analytics (UEBA): Eine Art von Cybersicherheitslösung bzw. eine Funktion, die Bedrohungen aufdeckt, indem sie vom Normalzustand (Baseline) abweichende Handlungen erkennt. UEBA kann für verschiedene Zwecke genutzt werden, kommt aber gewöhnlich zur Überwachung und Erkennung ungewöhnlicher Datenverkehrsmuster, unbefugter Datenzugriffe und -bewegungen oder verdächtiger oder bösartiger Aktivitäten in einem Computernetzwerk oder an Endpunkten zum Einsatz.

User Datagram Protocol (UDP): Ein Netzwerkprotokoll, das weder die Paketzustellung noch die Reihenfolge der Paketzustellung über ein Netzwerk garantiert.

Virtual Private Network (VPN): Ein VPN stellt eine private Verbindung zum Internet her, die als *Tunnel* bezeichnet wird. Alle von einem mit dem VPN verbundenen Gerät gesendeten Informationen werden verschlüsselt und durch diesen Tunnel geleitet. Wenn ein Gerät mit einem VPN verbunden ist, verhält es sich so, als ob es sich in demselben lokalen Netzwerk wie das VPN befindet. Das VPN leitet den Traffic vom Gerät durch seine sichere Verbindung zu und von der gewünschten Website bzw. dem Netzwerk weiter.

Voice over Internet Protocol (VoIP): Telefonieprotokolle, die für den Transport von Sprachkommunikation über TCP/IP-Netzwerke ausgelegt sind. *Siehe auch* Transmission Control Protocol (TCP) *und* User Datagram Protocol (IP).

VoIP: *Siehe* Voice over Internet Protocol (VoIP).

VPN: *Siehe* Virtual Private Network (VPN).

WAN: *Siehe* Wide Area Network (WAN).

Wide Area Network (WAN): Ein Computernetzwerk, das sich über ein weites geografisches Gebiet erstreckt und mehrere lokale Netzwerke (LANs) verbinden kann. *Siehe auch* Local Area Network (LAN).

Zero Trust: Zero Trust ist eine strategische Initiative, die Sicherheitsverletzungen verhindert, indem sie das Konzept des Vertrauens aus der Netzwerkarchitektur von Unternehmen verbannt. Zero Trust basiert auf dem Grundsatz „Niemals vertrauen, immer überprüfen" und soll die laterale Ausbreitung von Angriffen verhindern.

Zero Trust Network Access (ZTNA): Ein Sicherheitsansatz nach dem Prinzip „Niemals vertrauen, immer überprüfen", der die Benutzeridentität durch Authentifizierung und Attributüberprüfung verifiziert, bevor der Zugriff auf Anwendungen und Daten in der Cloud oder im Rechenzentrum gewährt wird.

ZTNA: *Siehe* Zero Trust Network Access (ZTNA) .

Zero Trust with Zero Exceptions

ZTNA 1.0 is over. Secure the future of hybrid work with ZTNA 2.0. Only available with Prisma® Access.

Palo Alto Networks Prisma® Access protects the hybrid workforce with the superior security of ZTNA 2.0 while providing exceptional user experiences from a simple, unified security product. Purpose-built in the cloud to secure at cloud scale, only Prisma Access protects all application traffic with best-in-class capabilities while securing both access and data to dramatically reduce the risk of a data breach.

Learn how Prisma Access secures today's hybrid workforce without compromising performance, backed by industry-leading SLAs to ensure exceptional user experiences.

https://www.paloaltonetworks.com/sase/ztna

Heute mit ZTNA beginnen

Hybride Belegschaften und Direct-to-App-Architekturen haben herkömmliche Sicherheitslösungen obsolet gemacht und die Angriffsfläche exponentiell vergrößert. Während die Häufigkeit und Komplexität von Bedrohungen zunimmt, werden betriebliche Abläufe durch die Nutzung vieler unterschiedlicher Sicherheitstools immer komplizierter. Bestehende cloudbasierte Sicherheitslösungen bieten zu viel Zugang und zu wenig Schutz. Sie gewährleisten keine konsistente und vollständige Sicherheit für alle Anwendungen und bieten eine unbefriedigende Performance und Benutzererfahrung. Zero Trust Network Access 2.0 ist der Weg in die Zukunft.

Im Buch ...

- Anwendungsfälle, die einen erfolgreichen Einstieg in ZTNA 2.0 illustrieren
- Unterschiede zwischen veralteten ZTNA-Lösungen und ZTNA 2.0
- Die fünf Grundsätze von ZTNA 2.0
- Fragen, die Sie Ihrem ZTNA-Anbieter stellen sollten
- Wie eine einheitliche Lösung eine außergewöhnliche Benutzererfahrung bieten kann

paloalto® NETWORKS

Lawrence Miller diente als Chief Petty Officer in der US-Navy und ist seit über 25 Jahren in verschiedenen Branchen im IT Bereich tätig. Er ist Mitautor des Buches *CISSP Für Dummies* und hat über 200 weitere *Für-Dummies*-Bücher zu zahlreichen technischen und sicherheitsbezogenen Themen verfasst.

Besuchen Sie Dummies.com®
für Schritt-für-Schritt-Anweisungen mit Bildern, Kurzanleitungen oder andere Bücher!

ISBN: 978-1-394-18374-6
Nicht für den Wiederverkauf

für dummies®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.