ZK RESEARCH
Influence and insight
through social media

Juli 2022

Hybride Arbeitsmodelle erfordern

ZTNA 2.0.

WHITEPAPER

Von
Zeus Kerravala

ZK Research
A Division of
Kerravala Consulting

ÜBER DEN AUTOR

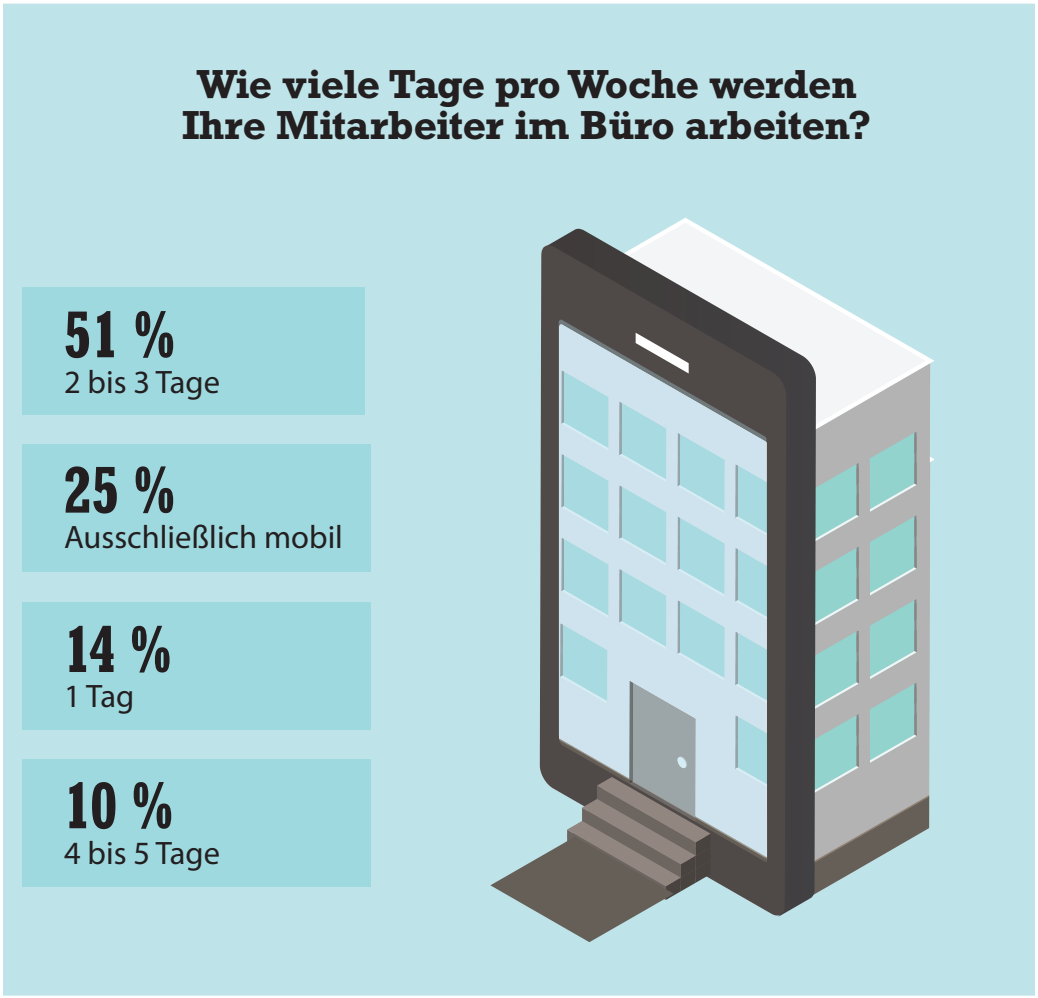
Zeus Kerravala ist der Gründer und Principal Analyst von ZK Research. Kerravala bietet taktische und strategische Empfehlungen, um seine Kunden sowohl in der aktuellen Wirtschaftslage als auch bei langfristigen Zielen zu unterstützen. Er stellt Forschungsergebnisse und Erkenntnisse für folgende Berufsgruppen bereit: IT- und Netzwerkmanager, Anbieter von IT-Hardware, -Software und -Services sowie Personen aus dem Finanzsektor, die in Unternehmen in diesen Märkten investieren möchten.

EINLEITUNG: HYBRIDE ARBEITSMODELLE SIND INZWISCHEN DIE NORM

Die COVID-19-Pandemie hat die Welt grundlegend verändert. Unternehmen mussten Pläne für die Digitalisierung, die auf mehrere Jahre ausgelegt waren, innerhalb weniger Monate umsetzen. Mitarbeiter, die bisher an einen Standort gebunden waren, können jetzt überall arbeiten – und dieser Trend wird sich auch weiterhin fortsetzen. Laut der Studie von ZK Research zum mobilen Arbeiten (Work-from-Anywhere Study 2022) haben vor der Pandemie nur 22 % der Beschäftigten regelmäßig extern gearbeitet, aber inzwischen sind 51 % zwei bis drei Tage und 14 % einen Tag pro Woche im Homeoffice (Abbildung 1). Das zeigt: Hybriden Arbeitsmodellen gehört die Zukunft.

Viele Unternehmen gehen nicht davon aus, dass ihre Mitarbeiter wieder in Vollzeit ins Büro zurückkehren werden. Brent Hyder, President und Chief People Officer bei Salesforce, berichtete MarketWatch, dass das Unternehmen seine Gebäude umgestalten und zahlreiche Schreibtische ausmustern wird. Er erwartet, dass 65 % der 54.000 Mitarbeiter nur zwischen ein und drei Tagen pro Woche im Büro arbeiten werden (im Vergleich zu 40 % vor der Pandemie). Auch andere Unternehmen wie Microsoft und Google bieten hybride Arbeitsmodelle an.

Abbildung 1: Hybriden Arbeitsmodellen gehört die Zukunft.



ZK Research, Work-from-Anywhere Study 2022

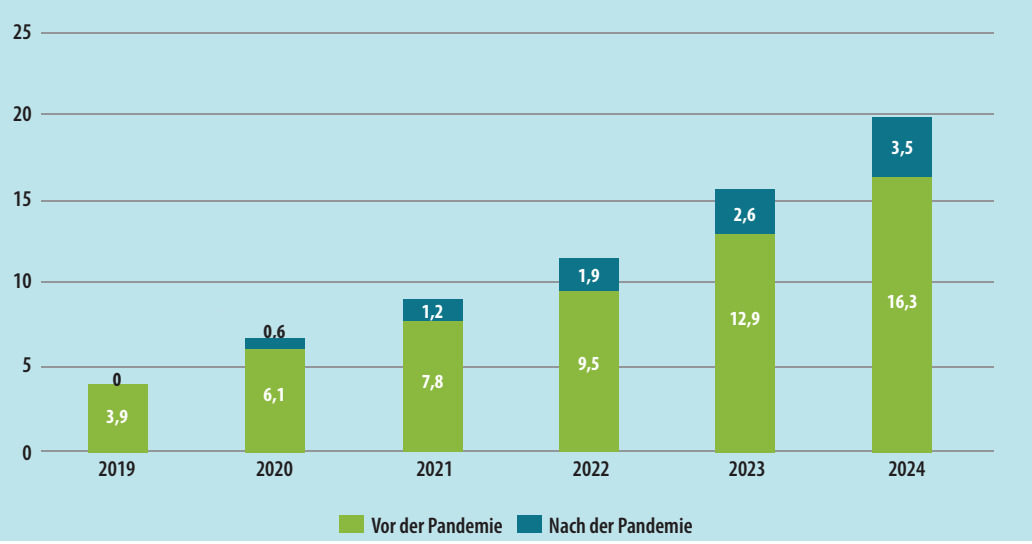
In den Medien wurde bereits ausführlich darüber berichtet, inwiefern hybride Arbeitsmodelle die Arbeitsweise der Menschen verändert haben, insbesondere in Bezug auf die Zusammenarbeit. Weniger bekannt sind hingegen die Folgen für die Unternehmens-IT. Hybride Arbeitsmodelle haben entscheidenden Einfluss auf die verwendeten Technologien und deren Bereitstellung. Einige Beispiele:

Die Cloud-Migration wurde beschleunigt und die Cloud-Modelle verändern sich. Bei den Cloud-Umgebungen findet ein Wechsel von einem zentralen zu einem verteilten Modell statt. Das heißt, Workloads und Anwendungen können in privaten oder öffentlichen Clouds und an Edge-Standorten genutzt werden. Cloud-Services sind standortunabhängig und damit ideal für hybride Arbeitsmodelle. Laut der Work-from-Anywhere Study 2022 von ZK Research haben 64 % der Unternehmen ihre Ausgaben für öffentliche Clouds erhöht und 58 % das Budget für private Clouds vergrößert.

Der Remotezugriff muss verändert werden. Unternehmen müssen sich darauf vorbereiten, dass die meisten Beschäftigten langfristig mobil arbeiten werden. VPNs (Virtual Private Networks) dienten als Übergangslösung, damit sich Mitarbeiter von externen Standorten aus verbinden konnten. Doch diese sind aufgrund von Sicherheitsproblemen, wie dem offenen Netzwerkzugang und Leistungseinbußen durch die Umleitung des Netzwerktraffics über das Rechenzentrum, langfristig nicht tragbar. Unternehmen werden daherSoftware-Defined Wide-Area Network (SD-WAN)- undSecure Access Service Edge (SASE)-Lösungen anschaffen, um sichere Verbindungen für mobile Mitarbeiter bereitstellen zu können. In Abbildung 2 ist der Anstieg an SD-WAN-Ausgaben aufgrund der Pandemie zu sehen.

Das IT-Team hat weniger direkte Kontrolle über die Infrastruktur. Vor zehn Jahren konnten IT-Teams noch feststellen, welche Endpunkte und Apps genutzt wurden, wo und wann auf Ressourcen zugegriffen wurde und wie Mitarbeiter ihre Verbindungen herstellten. Außerdem war das Netzwerk privat. Inzwischen haben sie deutlich weniger Kontrolle. Da viele Abteilungen eigene Software as a Service (SaaS)-Angebote anschaffen, ist eine Schatten-IT entstanden, durch SD-WAN wurde öffentliches Breitband eingebunden und hybride Arbeitsplätze haben den Perimeter des Unternehmens bis an das Homeoffice verschoben.

Abbildung 2: Anstieg der Ausgaben für SD-WAN



ZK Research, SD-WAN Forecast 2021

Zum Schutz der modernen hybriden Arbeitsplätze müssen Unternehmen den Zero-Trust-Ansatz überdenken und auf ZTNA 2.0 setzen.

Statt einer strikt kontrollierten Umgebung muss das IT-Team jetzt eine chaotische und unvorhersehbare Infrastruktur verwalten.

Von allen IT-Bereichen wird die Sicherheit davon am stärksten beeinträchtigt. Cybersicherheitsexperten müssen eine dynamische, verteilte und kurzlebige Angriffsfläche schützen. Dazu reichen herkömmliche Sicherheitsstrategien nicht mehr aus. VPNs galten jahrzehntelang als Standard, aber sie können die modernen Leistungs- und Sicherheitsanforderungen nicht erfüllen. Aus diesem Grund ist jetzt der richtige Zeitpunkt für den Wechsel zu einem Zero-Trust-Modell. Die erste Generation der Zero-Trust Network Access (ZTNA)-Lösungen bestand allerdings aus relativ simplen Tools für den Netzwerkzugriff mit einigen zusätzlichen Funktionen. Zum Schutz der modernen hybriden Arbeitsplätze müssen Unternehmen den Zero-Trust-Ansatz überdenken und auf ZTNA 2.0 setzen.

KAPITEL II: MIT ZTNA 1.0-LÖSUNGEN SIND UNTERNEHMEN ANFÄLLIGER

Das Interesse an ZTNA hat in den letzten Jahren stark zugenommen, da die Angriffsfläche verkleinert und somit die Sicherheit verbessert werden kann. IP-Netzwerke waren auf Offenheit ausgelegt, damit die Endpunkte untereinander Verbindungen herstellen konnten. Aus diesem Grund funktioniert das Internet so nahtlos und schnell. Es gibt jedoch ein Problem: Hat sich ein Angreifer erst einmal Zugang zu einem Netzwerk verschafft, kann er anschließend auf alle Unternehmensressourcen zugreifen und seine Aktivitäten oft monatelang in der Umgebung verbergen. Der Schaden für das betroffene Unternehmen ist immens.

Mit ZTNA soll ein Least-Privilege-Modell eingeführt werden, bei dem die Endpunkte nur dann miteinander kommunizieren können, wenn dies ausdrücklich genehmigt wurde. Dadurch ist die Angriffsfläche kleiner und Angreifer können auf nur wenige oder sogar gar keine anderen Systeme zugreifen – was ihren Aktionsradius und damit auch den Schaden erheblich einschränkt. Trotz dieses ZTNA-Konzepts wiesen die Lösungen der ersten Generation einige Beschränkungen auf:

Verstoß gegen das Least-Privilege-Prinzip: Das Least-Privilege-Prinzip ist das Herzstück von ZTNA, kann aber mit Netzwerklösungen nicht umgesetzt werden. Selbst wenn Anbieter behaupten, Kontrolle über die Anwendungen oder den Zugriff auf Anwendungsebene zu bieten, meinen viele damit Netzwerkkonstrukte wie IP-Adressen, Portnummern und FQDNs (Fully Qualified Domain Names). Das mag auf den ersten Blick sinnvoll erscheinen, da das Internet aus diesen Komponenten zusammengesetzt ist, führt aber zu drei großen Problemen:

- **Die Angriffsfläche ist zu groß.** Die meisten Anwendungen nutzen dynamische Ports und IP-Adressen. Aus diesem Grund müssen ZTNA-Lösungen den Zugriff auf zahlreiche unterschiedliche Ports und Adressen zulassen. Dadurch ist allerdings die Angriffsfläche wesentlich größer als eigentlich notwendig.
- **Der Zugriff kann nur auf Anwendungsebene beschränkt werden.** ZTNA 1.0-Lösungen kontrollieren nur die Anwendungsebene und können daher nicht den Zugriff auf Apps verhindern. In einigen Fällen kann es aber sinnvoll sein, den Zugriff auf bestimmte Funktionen zu beschränken. Doch dazu müsste die ZTNA-Lösung den Zugriff auf einer niedrigeren Ebene kontrollieren.
- **Es droht die Ausbreitung von Malware in der Umgebung.** Malware nutzt häufig dieselben Portnummern und/oder IP-Adressen wie legitime Anwendungen. So kann sie in die Umgebung eindringen und sich dann im Unternehmensnetzwerk ausbreiten.

Die Vorteile von ZTNA sind durchaus bekannt, doch die Lösungen der ersten Generation können diese nicht liefern.

Voraussetzung der Vertrauenswürdigkeit nach Gewährung des Zugriffs: Ein entscheidender Nachteil der ZTNA 1.0-Lösungen ist, dass Verbindungen, die für einen Benutzer oder eine Anwendung zugelassen wurden, vorbehaltlos als vertrauenswürdig eingestuft werden. Es wird davon ausgegangen, dass sich der Benutzer oder die Anwendung langfristig als vertrauenswürdig erweist. Allerdings treten Sicherheitsverletzungen immer erst nach der Gewährung des Zugriffs auf. Bei verdächtigen Verhaltensweisen muss daher der Zugriff widerrufen werden können. Mit dem Ansatz „Zulassen und ignorieren" der ZTNA 1.0-Lösungen ist dies aber nicht möglich.

Mangel an kontinuierlichen Sicherheitsprüfungen: ZTNA 1.0 wurde als Mechanismus für die Zugriffskontrolle entwickelt und verfügt nicht über die notwendigen Funktionen, um Malware zu erkennen oder abzuwehren oder die Ausbreitung im Netzwerk zu verhindern, nachdem der Zugriff auf eine App gewährt wurde. Das folgt letztendlich dem Security-through-Obscurity-Ansatz. Es wird allgemein davon ausgegangen, dass zugelassener Datenverkehr keine Malware oder sonstigen Bedrohungen enthält.

Kein Datenschutz: Die vorhandenen ZTNA-Lösungen bieten keinen Überblick und damit auch keine Kontrolle über Daten. Dadurch sind Unternehmen dem Risiko der Datenausschleusung durch Angreifer oder böswillige Insider ausgesetzt. Letzteres wird von Unternehmen häufig ignoriert, ist aber relativ oft die Ursache für Datenverlust. Laut dem Verizon Data Breach Investigations Report 2021 gab es zwischen 2018 und 2020 47 % mehr Sicherheitsvorfälle aufgrund von Insiderbedrohungen und diese machten 22 % aller Sicherheitsvorfälle aus.

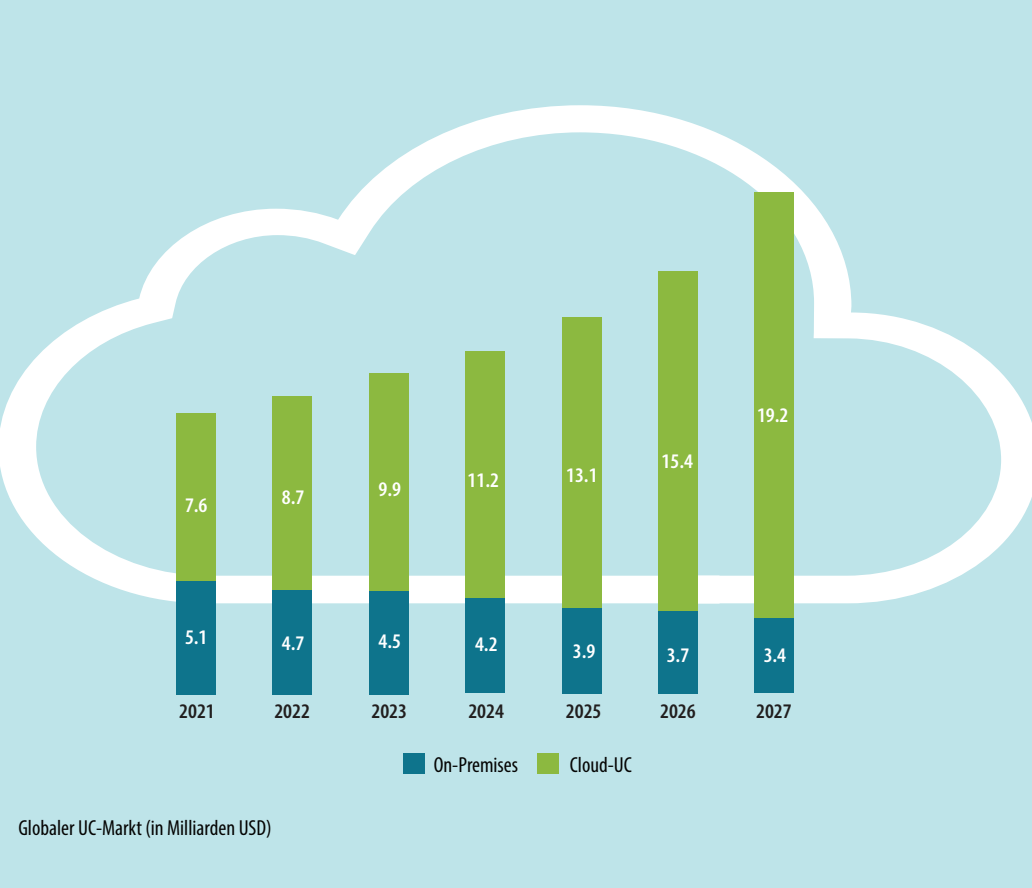
Kein umfassender Schutz aller Anwendungen: Die vorhandenen ZTNA-Lösungen decken nur den Teil der privaten Anwendungen ab, die statische Ports verwenden. Auch auf Microservices basierende cloudnative Anwendungen, Apps, die dynamische Ports nutzen, wie Sprach- und Videoanwendungen, oder serverbasierte Apps wie Helpdesk- und Patching-Systeme, können nicht zuverlässig geschützt werden. SaaS-Anwendungen werden von den vorhandenen ZTNA-Lösungen vollständig ignoriert, obwohl sie inzwischen den Großteil der Unternehmensanwendungen ausmachen und auch in Zukunft weiter an Bedeutung zunehmen werden. Laut dem Global UC Forecast 2021 von ZK Research wird die Zahl der Cloud-UC-Lösungen, einschließlich Sprach- und Videoanwendungen, bis 2026 mit einer durchschnittlichen jährlichen Wachstumsrate (CAGR) von 21 % steigen (Abbildung 3). Es ist eines der am schnellsten wachsenden Anwendungssegmente – und zeigt eine erhebliche Schwachstelle bei den ZTNA 1.0-Lösungen auf.

Die Vorteile von ZTNA sind durchaus bekannt, doch die Lösungen der ersten Generation können diese nicht liefern. Hybride Arbeitsmodelle haben die Arbeitsweise, die Wahl der Anwendungen und den Zugriff auf Umgebungen grundlegend verändert. Die ZTNA-Strategie muss daher endlich weiterentwickelt werden.

KAPITEL III: WAS IST ZTNA 2.0?

Mit ZTNA 2.0 wird das Zugriffsmanagement ganz neu gestaltet. Die Lösungen der ersten Generation waren VPN-Produkte mit Zusatzfunktionen, aber die zweite Generation wird von Grund auf neu entwickelt, damit das Least-Privilege-Prinzip konstant im gesamten Unternehmen durchgesetzt werden kann.

Abbildung 3: Mit der Zunahme an hybriden Arbeitsmodellen steigt auch die Zahl der Cloud-Kommunikationslösungen.



ZK Research, Global UC Forecast 2022

Bei ZTNA 2.0 wurden die folgenden Prinzipien berücksichtigt:

Fokus auf der Anwendungsebene: Mit ZTNA 2.0 wechselt der Fokus vom Netzwerk (Layer 3) auf die Anwendungen (Layer 7), sodass das Potenzial der Zero-Trust-Strategie vollständig ausgeschöpft werden kann. Auf diese Weise können präzise Zugriffskontrollen auf Anwendungsebene und sogar niedrigeren Ebenen und unabhängig von den Netzwerkkonfigurationen durchgeführt werden. Wenn ein Benutzer seinen Standort wechselt oder Netzwerkänderungen vorgenommen werden, sind diese für ZTNA einsehbar. Damit wird das Least-Privilege-Prinzip konstant durchgesetzt.

Kontinuierliche Prüfung der Vertrauenswürdigkeit: Wie schon im vorherigen Kapitel angemerkt, sind langfristige Vertrauensbeziehungen eigentlich keine Lösung. Wenn eine Verbindung grundsätzlich als vertrauenswürdig eingestuft wird, nachdem einem Benutzer der Zugriff auf eine Anwendung gewährt wurde, werden unter Umständen Sicherheitsvorfälle und Datenlecks übersehen. Bei ZTNA 2.0 müssen die Vertrauensbeziehungen kontinuierlich überprüft und Änderungen des Geräte- und Benutzerverhaltens oder der Anwendungsaktivitäten berücksichtigt werden. Bei Anomalien wird der Zugriff widerrufen. Meldet sich ein Benutzer beispielsweise wenige Minuten nach dem lokalen Zugriff auf eine App plötzlich

ZTNA 2.0 ermöglicht die konsistente Kontrolle der Daten in allen im Unternehmen genutzten Anwendungen.

von einem Standort am anderen Ende der Welt an, wurden seine Anmeldedaten höchstwahrscheinlich gestohlen. Ebenso verdächtig ist eine Anwendung, die plötzlich einen neuen Port verwendet. Das kann darauf hindeuten, dass sie manipuliert wurde.

Kontinuierliche Sicherheitsprüfungen: ZTNA 2.0-Lösungen sollten kontinuierlich eine Deep Packet Inspection (DPI) des gesamten Datenverkehrs durchführen, auch für Verbindungen, die bereits zugelassen wurden. Auf diese Weise können sowohl Sicherheitsvorfälle als auch Zero-Day-Bedrohungen schnell erfasst und abgewehrt werden. Kontinuierliche Sicherheitsprüfungen sind außerdem die beste Abwehrmethode, wenn die Anmeldedaten legitimer Benutzer gestohlen und für Angriffe auf Anwendungen oder Infrastrukturen ausgenutzt werden.

Umfassender Datenschutz: ZTNA 2.0 ermöglicht die konsistente Kontrolle der Daten in allen im Unternehmen genutzten Anwendungen, einschließlich On-Premises-Anwendungen und SaaS-Apps. Letztere können mit Lösungen der ersten Generation nicht überprüft werden. Für all dies wird nur eine einzigeData Loss Prevention (DLP)-Richtlinie benötigt, was die Abläufe erheblich vereinfacht.

Umfassende Anwendungssicherheit: Mit ZTNA 2.0 sind alle Anwendungen im Unternehmen sicher – von veralteten Anwendungen über SaaS- und private Apps bis zu modernen, cloudnativen Anwendungen. Erwähnenswert ist, dass dies auch für Anwendungen gilt, die dynamische Ports und serverbasierte Verbindungen nutzen.

KAPITEL IV: PALO ALTO NETWORKS BIETET EINE UMFASSENDE ZTNA 2.0-LÖSUNG

Palo Alto Networks ist Marktführer in der Sicherheitsbranche. Das Unternehmen mit Sitz im kalifornischen Silicon Valley bietet das umfassendste und vielfältigste Produktportfolio aller Sicherheitsanbieter. Seine Lösung Prisma Access hat sich im Laufe der Jahre zum De-Facto-Standard für den Schutz und die Anbindung mobiler Mitarbeiter entwickelt. Palo Alto Networks hat schon sehr früh eine ZTNA-Lösung auf den Markt gebracht und wurde im aktuellen New Wave-Bericht von Forrester zu ZTNA als „Leader" ausgezeichnet.

Kürzlich hat das Unternehmen die branchenweit erste ZTNA 2.0-Lösung auf Prisma Access vorgestellt – ein anwenderfreundliches und einheitliches Sicherheitsprodukt für den Schutz mobiler Mitarbeiter. Zwar behaupten viele Anbieter, Cloud-Sicherheit zu bieten, doch die meisten Produkte basieren auf älteren Technologien, die nur mit dem Lift-and-Shift-Ansatz migriert wurden. Palo Alto Networks hingegen bietet umfassend modernisierte, cloudnative Sicherheitsservices, einschließlich SWG (Secure Web Gateway), NG-CASB (Next-Generation Cloud Access Security Broker), FWaaS (Firewall as a Service) und DLP auf einer cloudnativen globalen Edge-Plattform. Mit einem einheitlichen Richtliniensystem und der Verwaltung über eine zentrale Managementkonsole sorgt Prisma Access für zuverlässigen Schutz moderner hybrider Arbeitsumgebungen ohne Abstriche bei der Leistung.

Prisma Access von Palo Alto Networks erfüllt auch die in Kapitel III aufgeführten Kriterien:

Least-Privilege-Prinzip: Prisma Access deckt Layer 3 bis 7 des Open Systems Interconnection (OSI)-Stacks ab – von der Netzwerk- bis zur Anwendungsebene. Palo Alto Networks setzt patentierte App-ID-Technologie ein, um den Zugriff auf Anwendungen und Anwendungsfunktionen strikt zu kontrollieren.

Prisma Access nutzt eine einheitliche Lösung zum Schutz aller Benutzer und Anwendungen im gesamten Unternehmen.

Dazu gehören auch die Kontrolle spezifischer Funktionen wie das Hoch- oder Herunterladen.

Kontinuierliche Prüfung der Vertrauenswürdigkeit: Die Lösung von Palo Alto Networks überprüft fortlaufend die Vertrauenswürdigkeit mithilfe der folgenden drei patentierten Prozesse:

- **User-ID** bietet einen umfassenden Überblick über die Benutzer und überwacht deren Verhalten kontinuierlich auf verdächtige Aktivitäten.
- **Device-ID** bietet einen Überblick über den Gerätestatus und ermöglicht auch das Widerrufen des Zugriffs, falls ein Gerät gegen die Unternehmensrichtlinien verstößt.
- **App-ID** sorgt dafür, dass der Netzwerktraffic auf bestimmten Ports nur von zulässigen Anwendungen stammt. So wird beispielsweise Port 443 nur für sicheren Webtraffic genutzt.

Kontinuierliche Sicherheitsprüfungen: Die Engine für maschinelles Lernen (ML) von Prisma Access kann 95 % der Bedrohungen inline und ohne Signaturen abwehren. Dank der ML-Funktionen und der Cloud Security Services von Palo Alto Networks können jeden Tag mehr als 224 Milliarden Bedrohungen blockiert werden. Für Bedrohungen, die sich durch Inline-Schutz nicht verhindern lassen, nutzt Prisma Access die Single-Pass-Prüfung des Datenverkehrs weiterer Cloud-Delivered Security Services. Dazu gehören:

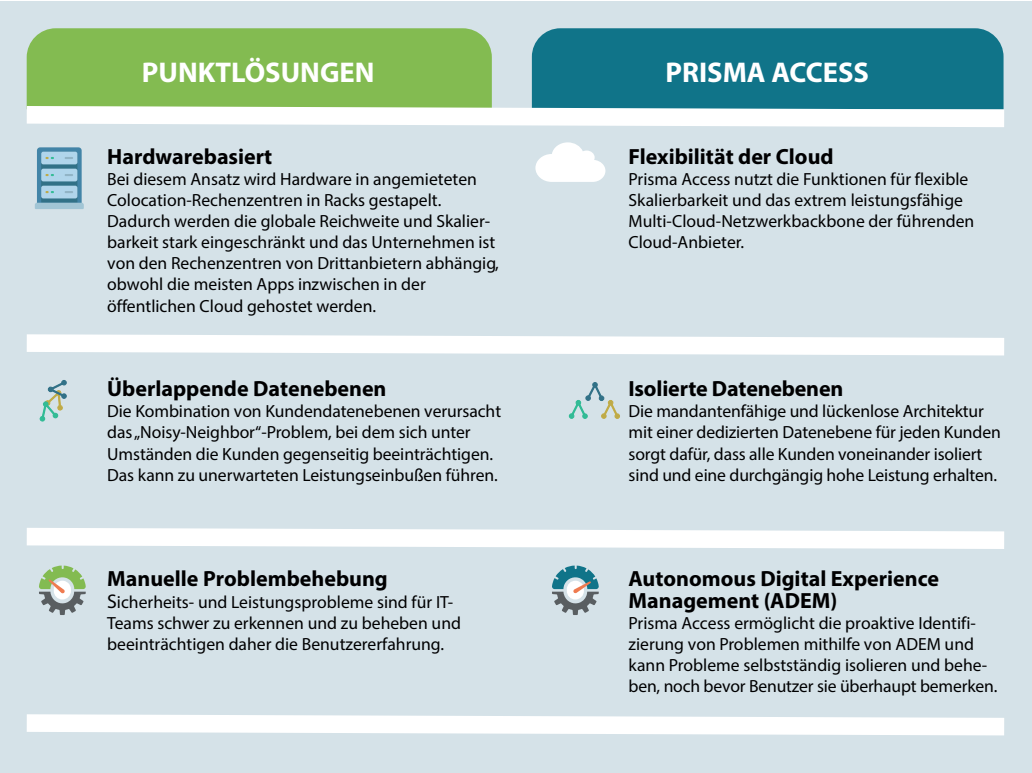
- **Threat Prevention** verhindert Exploits, Command-and-Control-Verbindungen und andere Netzwerkangriffe für alle Apps und Protokolle.
- **WildFire** ist ein riesiges Malwareanalysesystem, das eine schnelle Signaturbereitstellung ermöglicht.
- **Advanced URL Filtering** ist ein Websicherheitsservice, der 24 % mehr Phishingangriffe als die Lösungen anderer Anbieter abwehrt.
- **DNS Security** verhindert alle großen Angriffe aufDomain Name System (DNS)-Ebene.

Schutz aller Daten: Im Gegensatz zu ZTNA 1.0-Lösungen, die Datenausschleusungen oder -verluste nicht erkennen können, unterstützt Prisma Access Enterprise DLP von Palo Alto Networks, das einen konsistenten Überblick über den Datenzugriff im gesamten Unternehmen bietet. Kunden können in einer zentralen Managementkonsole mit nur einer Richtlinie einheitliche DLP-Maßnahmen auf alle Daten anwenden – von veralteten On-Premises-Anwendungen über Apps in der öffentlichen Cloud bis zu SaaS-Anwendungen.

Schutz aller Anwendungen: Prisma Access nutzt eine einheitliche Lösung zum Schutz aller Benutzer und Anwendungen im gesamten Unternehmen, unabhängig davon, ob für die Verbindung ein Agent genutzt wird oder nicht. Geschützt werden sowohl On-Premises- und veraltete Anwendungen als auch Apps in öffentlichen Clouds und SaaS- und moderne cloudnative Anwendungen.

Außerdem wurde Prisma Access speziell für eine erstklassige Benutzererfahrung entwickelt. Palo Alto Networks bietet daher auch aggressive SLAs (Service-Level Agreements) mit einer Verfügbarkeit von 99,999 % und Sicherheitsverarbeitungszeiten unter 10 ms. Den Untersuchungen von ZK Research zufolge ist Palo Alto Networks der einzige ZTNA 2.0-Anbieter mit einem Leistungs-SLA für SaaS-Anwendungen von Drittanbietern.

Abbildung 4: Moderner ZTNA-Ansatz dank cloudnativer Prisma Access-Architektur



Palo Alto Networks und ZK Research, 2022

Sicherheitsteams könnten natürlich versuchen, eine ZTNA 2.0-Lösung aus diversen Punktlösungen zu erstellen und mithilfe eines Lift-and-Shift-Ansatzes in die Cloud zu migrieren, doch ein solches Modell weist im Vergleich zur cloudnativen Lösung Prisma Access von Palo Alto Networks deutliche Lücken auf. In Abbildung 4 sind die größten Unterschiede dieser beiden Ansätze aufgelistet.

KAPITEL V: FAZIT UND EMPFEHLUNGEN

Hybride Arbeitsmodelle sind aus dem Alltag nicht mehr wegzudenken und haben das Arbeitsleben grundlegend verändert. Aber dadurch ändern sich auch die Anforderungen der Unternehmen in Bezug auf den Schutz und die Konnektivität der Mitarbeiter. Ältere VPNs und ZTNA-Lösungen der ersten Generation reichten als Übergangslösung aus, um Benutzern grundlegende Verbindungen zu ermöglichen, aber jetzt sollten Unternehmen die langfristigen Auswirkungen der hybriden Arbeitsmodelle bedenken.

Die Art des Zugriffs muss sich verändern und ZTNA 2.0 ist die richtige Lösung. Die älteren Lösungen haben vor zehn Jahren gute Dienste geleistet, aber sie waren nie auf eine dynamische und verteilte Welt ausgelegt. ZTNA 2.0 wurde speziell für verteilte Cloud-First-Unternehmen entwickelt – und dazu gehört inzwischen die Mehrzahl der Unternehmen. Die Einführung von ZTNA 2.0 ist daher ein Muss. Unternehmen, die sich für ZTNA 2.0 interessieren, empfiehlt ZK Research Folgendes:

Passen Sie Ihre Sicherheitsmaßnahmen an die modernen hybriden Arbeitsmodelle an. Die Kombination von Punktlösungen hat in der Vergangenheit ausgereicht, da die IT-Teams die vollständige Kontrolle hatten – von den verwendeten Apps und Geräten bis zum Netzwerk und Netzwerkzugriff. Bei hybriden Arbeitsmodellen werden die Anwendungen in die Cloud verschoben, die Geräte werden mobil eingesetzt und die Mitarbeiter sitzen im Homeoffice. Punktlösungen haben daher ausgedient und es muss stattdessen eine Plattform eingeführt werden, die lückenlose Sicherheitsmaßnahmen ermöglicht. Prisma Access von Palo Alto Networks ist ein gutes Beispiel für eine solche Plattform.

Beginnen Sie mit dem größten Sicherheitsproblem. Alle Unternehmen sollten ZTNA 2.0 in Betracht ziehen, aber die Ausgangssituation wird sich im Einzelnen unterscheiden. ZK Research hat drei Bereiche ermittelt, die Unternehmen die Einführung von ZTNA erleichtern können:

- Schutz des Zugriffs auf private Apps als Ersatz für einen VPN
- Schutz des Internet- und SaaS-Zugriffs als Ersatz für SWG
- Implementierung moderner Sicherheitsfunktionen für SaaS-Apps als Ersatz für CASB und DLP

Wählen Sie einen cloudnativen Sicherheitspartner. Etliche Anbieter behaupten, Cloud-Sicherheit zu bieten. Kunden müssen sich daher bewusst sein, dass nicht alle Cloud-Umgebungen identisch sind und dass „Cloud“ auch nicht immer „cloudnativ“ bedeutet. Sie müssen darauf achten, dass der Anbieter eine moderne, cloudnative Plattform bereitstellt, die schnellere Innovationen und eine bessere Resilienz ermöglicht.

KONTAKT

zeus@zkresearch.com

Mobiltelefon: +1 301-775-7447

Büro: +1 978-252-5314