Enterprise Strategy Group | Getting to the bigger truth.™

ESG-WHITEPAPER

Die Weiterentwicklung von ZTNA zu umfassenden Zero-Trust-Strategien

Von John Grady, ESG Senior Analyst

Mai 2022

Dieses ESG-Whitepaper wurde von Palo Alto Networks in Auftrag gegeben und wird unter Lizenz von TechTarget, Inc vertrieben.

Inhalt

Kurzfassung

Der Zero-Trust-Netzwerkzugriff (Zero Trust Network Access, ZTNA) wurde während der Pandemie zu einer wichtigen Strategie, mit der Unternehmen ihren mobilen Arbeitern eine bessere Sicherheit, Verwaltung und Skalierung als in den vorhandenen virtuellen privaten Netzwerken (VPN) bieten konnten. Der Wechsel zu mobilen und hybriden Arbeitsmodellen hat auch weiterhin Folgen – nicht nur in Bezug auf den Arbeitsplatz, sondern auch auf die Arbeitsweise. Unsere Arbeit ist nicht mehr vorrangig standortgebunden, sondern orientiert sich stärker an den jeweiligen Aktivitäten. Die Unternehmen mussten sich erst auf dieses neue Hybridmodell einstellen, bei dem sich Benutzer und Anwendungen an diversen Standorten befinden können, und die IT-, Netzwerk- und Sicherheitsteams standen vor ganz neuen Herausforderungen, da sich die Angriffsfläche durch die direkten Verbindungen zu Anwendungen enorm vergrößerte.

Einige Unternehmen haben ZTNA-Lösungen implementiert, um die Infrastruktur zu modernisieren und die erforderlichen Netzwerk- und Sicherheitsfunktionen am Cloud-Service-Edge bereitzustellen, damit die direkten Verbindungen zwischen Benutzern und Anwendungen so kurz wie möglich sind. Doch die erste Generation dieser Lösungen (ZTNA 1.0) hat die Zero-Trust-Versprechen in vielen Punkten nicht erfüllt. Häufig gewährten sie deutlich mehr Zugriffsrechte als erwünscht. Außerdem werden die zugelassenen Verbindungen in ZTNA 1.0-Lösungen dauerhaft als vertrauenswürdig eingestuft, was mithilfe von komplexen Bedrohungen und/oder schädlichen Aktivitäten ausgenutzt werden kann.

Daher wird es Zeit für einen neuen ZTNA-Ansatz, der speziell auf die Anforderungen moderner Anwendungen und hybrider Arbeitsplätze sowie die Herausforderungen komplexer Bedrohungen ausgelegt ist. In diesem Whitepaper erläutern wir, warum ein neuer ZTNA-Ansatz notwendig ist, welche Funktionen benötigt werden (zum Beispiel die Einhaltung des Least-Privilege-Prinzips bei Zugriffsrechten und die kontinuierliche Überprüfung des Vertrauensverhältnisses), warum dabei Benutzeraktivitäten, Verhaltensweisen und der unternehmensweite Kontext wichtig sind sowie welche Sicherheitsprüfungen erforderlich sind, um alle Anwendungen und Daten an allen Orten effektiv zu schützen. Außerdem stellen wir den neuen ZTNA-Ansatz in der cloudbasierten Prisma Access-Lösung von Palo Alto Networks vor und geben Empfehlungen, wie Entscheidungsträger ZTNA 2.0-Technologien zur Risikominimierung an modernen Arbeitsplätzen einsetzen sollten.

Daher wird es Zeit für einen neuen ZTNA-Ansatz, der speziell auf die Anforderungen moderner Anwendungen und hybrider Arbeitsplätze sowie die Herausforderungen komplexer Bedrohungen ausgelegt ist.

Sicherer Zugriff wird an modernen Arbeitsplätzen zur Herausforderung

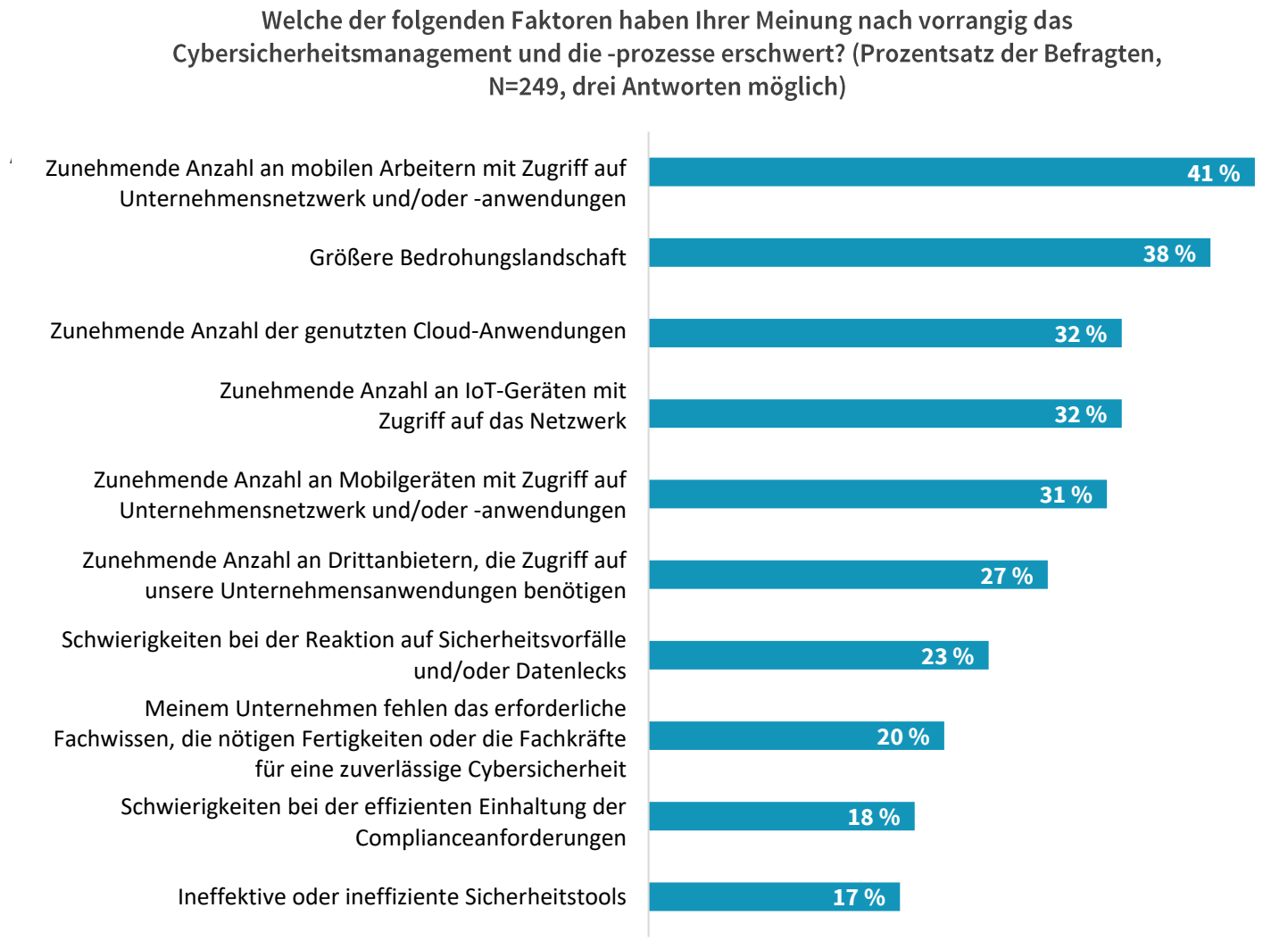
Die Pandemie hat gezeigt, dass mobile und hybride Arbeitsplätze nicht nur möglich sind, sondern auch von einem Großteil der Beschäftigten bevorzugt werden. Was als Notlösung in einer Krisensituation begann, hat sich zu einer Chance für Unternehmen entwickelt, die Effizienz und Produktivität zu steigern und besser auf die Bedürfnisse der Mitarbeiter einzugehen. Doch die Ausmaße und die Geschwindigkeit des Wechsels zu mobilen und hybriden Arbeitsmodellen haben IT-, Sicherheits- und Netzwerkteams vor große Herausforderungen gestellt. Laut einer Umfrage von ESG sind 59 Prozent der Entscheidungsträger der Meinung, dass es in den letzten zwei Jahren schwieriger geworden sei, für Cybersicherheit zu sorgen.[1]

Als größtes Problem nannten die Umfrageteilnehmer die zunehmende Anzahl der mobilen Arbeiter mit Zugriff auf Unternehmensnetzwerk und/oder -anwendungen. Zu den weiteren Faktoren gehörten die dynamische

[1] Quelle: ESG Survey Results, *The State of Zero Trust Security Strategies,* Mai 2021.

Bedrohungslandschaft, die zunehmende Anzahl an Cloud-Anwendungen im Unternehmen und der notwendige Zugriff von Drittanbietern auf die Unternehmensressourcen an (siehe Abbildung 1).[2]

Abbildung 1: Ursachen für Probleme bei der Cybersicherheit



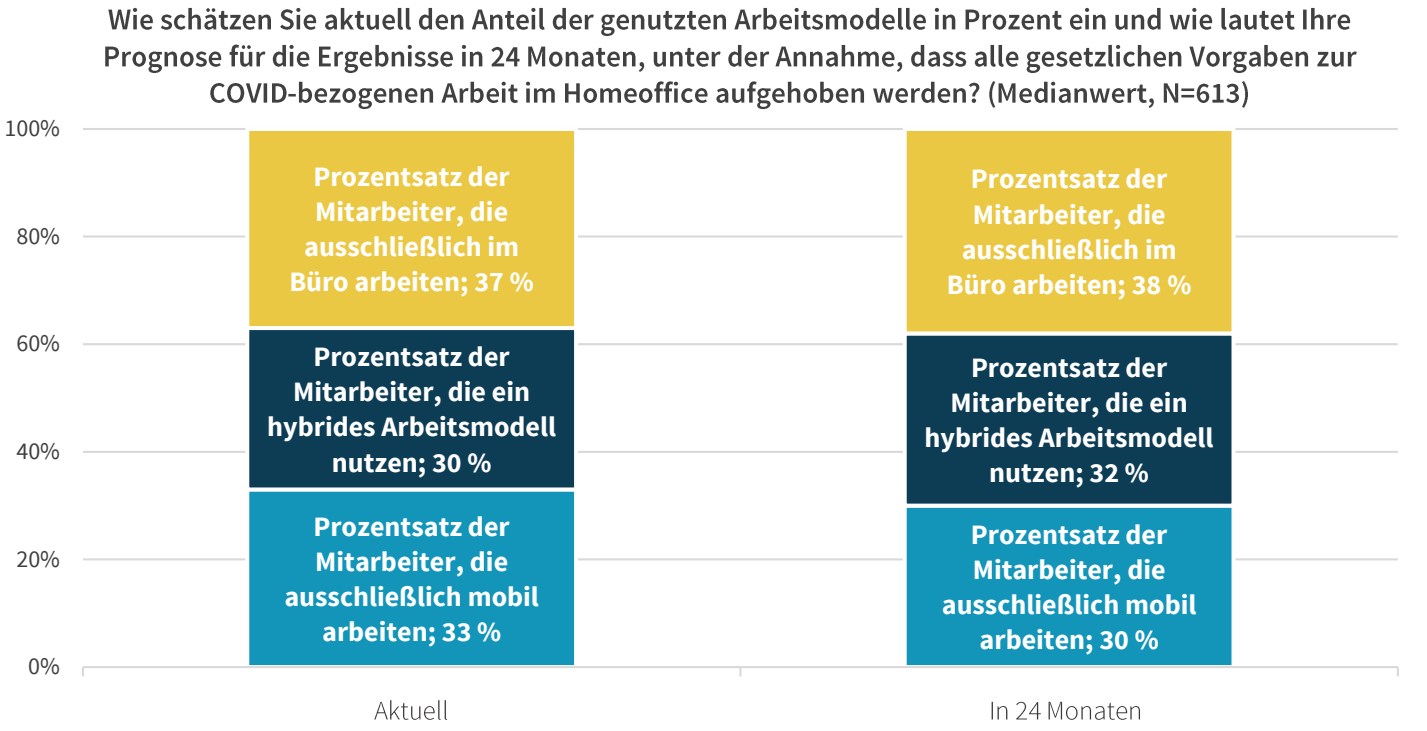
Quelle: ESG, a division of TechTarget, Inc.

Die Umstände haben sich inzwischen etwas verändert, aber die Folgen dieses Wechsels bleiben langfristig bestehen. Was als Notlösung gedacht war, hat sich zu einem neuen hybriden Arbeitsmodell entwickelt, das inzwischen von Mitarbeitern erwartet und häufig sogar gefordert wird. Eine Rückkehr zum Status quo vor der Pandemie ist weder realistisch noch rentabel. Laut einer Umfrage von ESG nutzen mehr als 60 Prozent der Beschäftigten inzwischen ein hybrides oder vollständig mobiles Arbeitsmodell. Schätzungen zufolge wird sich dieser Prozentsatz in den nächsten zwei Jahren kaum verändern (siehe Abbildung 2).[3]

[2] Ebd.

[3] Quelle: ESG Complete Survey Results, *2021 SASE Trends: Plans Coalesce But Convergence Will Be Phased,* Dezember 2021.

Abbildung 2: Gemischte Arbeitsmodelle sind die Zukunft



Quelle: ESG, a division of TechTarget, Inc.

Diese neue Arbeitswelt bringt neue Herausforderungen mit sich, zum Beispiel in Bezug auf den konsistenten Schutz von mobilen Arbeitern und den Zugriff auf das Unternehmensnetzwerk und geschäftskritische Anwendungen. Weitere Faktoren sind die wesentlich größere Angriffsfläche und der Wechsel von einer Infrastruktur, in der der gesamte Datenverkehr über das Unternehmensnetzwerk in ein Rechenzentrum geleitet werden muss, zu einem Modell mit überwiegend direkten Verbindungen zu Anwendungen und Edge-Computing.

Gleichzeitig werden Angreifer technisch immer versierter und können auf größere finanzielle Mittel zurückgreifen – in einigen Fällen werden sie sogar staatlich gesponsert. Außerdem nutzen Hacker gezielt Lücken in mobilen und hybriden Arbeitsmodellen und Schwachstellen in vorhandenen Netzwerk- und Sicherheitslösungen aus. Aus diesen Gründen wird es höchste Zeit für einen neuen Ansatz.

Das Zero-Trust-Prinzip und ZTNA

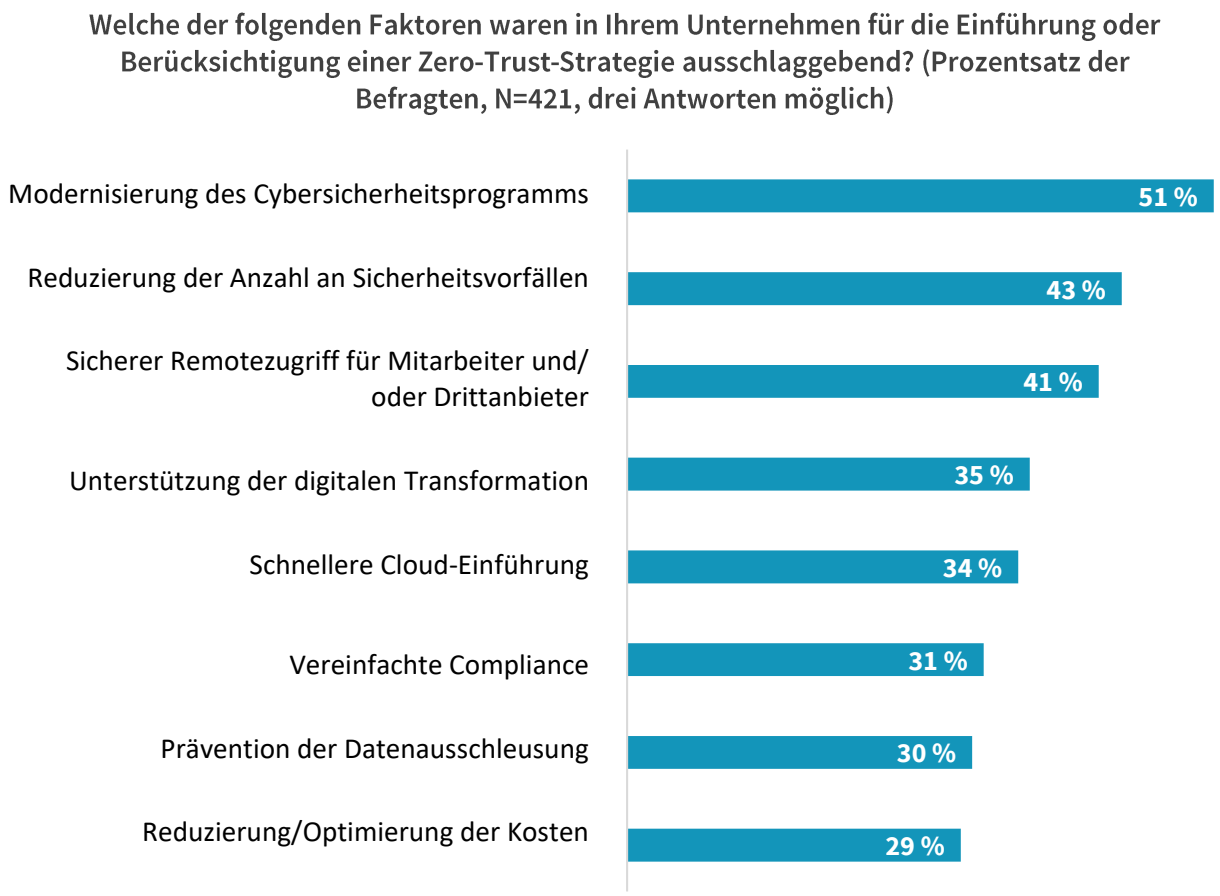
All diese Herausforderungen machen deutlich, dass das Zero-Trust-Prinzip und ZTNA unbedingt in einen neuen Netzwerk- und Sicherheitsansatz für hybride Arbeitsmodelle integriert werden müssen. Mit einer korrekt implementierten Zero-Trust-Strategie lassen sich die Risiken von Sicherheitsverletzungen verringern, die Richtlinienverwaltung und -durchsetzung vereinfachen und zusätzliche Schutzmaßnahmen für Benutzer, Anwendungen und Daten einrichten. Den Begriff „Zero Trust“ gibt es zwar schon seit 2010, aber die Umsetzung braucht Zeit. In einer Umfrage von ESG gaben 54 Prozent der Befragten an, dass ihre Zero-Trust-Initiative erst vor weniger als zwei Jahren eingeführt wurde.[4]

Es gibt verschiedene Gründe, weshalb sich Unternehmen für Zero-Trust-Strategien interessieren. Dazu gehören auch allgemeine IT-Ziele wie die Unterstützung der digitalen Transformation und eine schnellere Cloud-Einführung. Zwei der

[4] Quelle: ESG Survey Results, *The State of Zero Trust Security Strategies,* Mai 2021.

gängigsten Gründe sind die Modernisierung der Cybersicherheitsmaßnahmen und der sichere Remotezugriff für Mitarbeiter und Drittanbieter (siehe Abbildung 3).[5]

Abbildung 3: Ausschlaggebende Faktoren für die Einführung einer Zero-Trust-Strategie



Quelle: ESG, a division of TechTarget, Inc.

Die rasante Zunahme des mobilen Arbeitens während der Pandemie hat für zusätzliches Interesse und höhere Erwartungen an Zero-Trust-Strategien gesorgt. Da Unternehmen sehr schnell auf ein mobiles Arbeitsmodell umsteigen mussten, wurden die Nachteile von VPNs in Bezug auf die Leistung und den Remotezugriff allzu offensichtlich. Dazu gehören die fehlende Skalierbarkeit, die Abhängigkeit von hardwarebasierter Technologie, die notwendige Umleitung des Datenverkehrs über das Unternehmensnetzwerk und zu weitreichende Zugriffsrechte.

Diese Probleme gaben den entscheidenden Anstoß, und zwar nicht nur in Bezug auf Zero Trust als neue Strategie, sondern auch zur Einführung von ZTNA als praktische und weniger riskante Alternative zu VPNs. Laut einer ESG-Umfrage nutzen 69 Prozent der Unternehmen ZTNA und haben sich gegen VPN entschieden oder planen, ihr VPN zu ersetzen.[6] ZTNA bietet im Vergleich mit VPN deutliche Vorteile, zum Beispiel:

- Benutzer können nur die Anwendungen und Services sehen, für die ihnen Zugriffsrechte zugewiesen wurden.
- Anwendungen sind im öffentlichen Internet nicht sichtbar.
- Die meisten ZTNA-Lösungen werden in der Cloud bereitgestellt.

[5] Ebd.
[6] Quelle: ESG Complete Survey Results, *2021 SASE Trends: Plans Coalesce But Convergence Will Be Phased,* Dezember 2021.

Die vorhandenen ZTNA 1.0-Lösungen waren zwar schon eine erste Verbesserung zu den VPN-Appliances, doch durch die Zunahme der mobilen und hybriden Arbeitsplätze und hybriden Cloud-Umgebungen sowie die große Anzahl an modernen Anwendungen treten Schwachstellen zutage, die behoben werden müssen.

Gründe für einen neuen ZTNA-Ansatz

Was gibt es an den ZTNA 1.0-Lösungen auszusetzen? Die größten Probleme liegen in der Zugriffskontrolle, dem Least-Privilege-Zugriff, der unzureichenden Transparenz und dem „Zulassen-und-ignorieren"-Modell, das auf Vertrauensbeziehungen setzt, diese aber selten überprüft. Das bedeutet, dass die Zero-Trust-Prinzipien nicht in vollem Umfang beachtet oder durchgesetzt werden. Zu den Schwachstellen des ZTNA 1.0-Ansatzes gehören unter anderem:

1. Least-Privilege-Prinzip: ZTNA 1.0-Lösungen bieten keine detaillierten Zugriffskontrollen. Das verstößt gegen das Least-Privilege-Prinzip, da die Anwendungen als Netzwerkkonstrukt auf Layer 3 und 4 (IP und Port) betrachtet werden und die Benutzer mehr Zugriffsrechte als nötig erhalten. Außerdem wird der Kontext der Anwendungen nicht beachtet, der bei der Verifizierung von Benutzern oder Geräten helfen kann, zum Beispiel welche Anwendungen genutzt werden, zu welcher Tageszeit oder an welchem Ort.

2. „Zulassen und ignorieren": Nachdem der Zugriff auf eine Anwendung gewährt wurde, wird diese Verbindung dauerhaft als vertrauenswürdig eingestuft. Dabei wird davon ausgegangen, dass das Verhalten von Benutzer und Anwendung stets vertrauenswürdig ist. Das „Zulassen-und-ignorieren"-Modell eignet sich weder für moderne Unternehmensumgebungen noch für eine echte Zero-Trust-Strategie, da für Sicherheitsverletzungen auch legitime Aktivitäten ausgenutzt werden, die sich mit diesem Modell nicht verhindern lassen.

3. Keine Sicherheitsprüfungen: Aktuelle Lösungen gehen davon aus, dass der Datenverkehr sicher ist, ohne ihn zu überprüfen, und verfügen auch nicht über die notwendigen Funktionen, um Malware zu erkennen oder abzuwehren oder die Ausbreitung im Netzwerk zu verhindern, wenn der Zugriff auf eine Anwendung erst einmal gewährt wurde. Sie können Zugriff gewähren, aber bieten keinen Überblick und keine Kontrolle über den Datenverkehr, sodass das Unternehmen einem höheren Risiko in Bezug auf Datenlecks ausgesetzt ist.

4. Begrenzter oder fehlender Datenschutz: Die aktuellen Lösungen bieten kaum Überblick oder Kontrolle über sensible Daten. Erschwerend hinzu kommt, dass Unternehmen oft verschiedene Lösungen für den Schutz sensibler Daten in privaten und SaaS- oder Internetanwendungen nutzen. Dadurch entstehen verteilte, isolierte Infrastrukturen, die für zusätzliche Komplexität sorgen und das Risiko der Datenausschleusung von Angreifern oder böswilligen Insidern erhöhen. Unternehmen müssen stets die Kontrolle über ihre Daten in allen Anwendungen haben und sollten dazu nur eine Richtlinie zum Schutz vor Datenverlust benötigen.

5. Separate Plattformen für Cloud- und On-Premises-Anwendungen: Laut einer ESG-Umfrage ist die Abdeckung von Cloud- und On-Premises-Umgebungen der wichtigste Punkt für Unternehmen bei der Wahl der Zero-Trust-Technologien.[7] Viele vorhandene ZTNA-Lösungen wurden entweder für On-Premises-Anwendungen oder für Cloud-Anwendungen entwickelt, nicht aber für beide Varianten. Ein moderner Ansatz muss alle Anwendungen abdecken, um die Komplexität und die Risiken zu minimieren.

[7] Quelle: ESG Survey Results, *The State of Zero Trust Security Strategies,* Mai 2021.

Wichtige Voraussetzungen für unternehmensweiten ZTNA

Damit Unternehmen die Herausforderungen der neuen Arbeitsmodelle bewältigen können, müssen die ZTNA-Lösungen diese Lücken schließen. Andernfalls investieren die Unternehmen in Lösungen, die nicht das erforderliche Maß an Sicherheit bieten. Abgesehen von den höheren und unnötigen Risiken müssen Entscheidungsträger bei der Auswahl auch das Nutzererlebnis, die Leistungsfähigkeit und die einfache Verwaltung berücksichtigen. Zu den wichtigsten Anforderungen an die nächste Generation der ZTNA-Lösungen, die die Herausforderungen hybrider Arbeitsmodelle, hybrider Cloud-Umgebungen und moderner Anwendungen berücksichtigen, gehören unter anderem:

- Ausrichtung auf Anwendungen: Sie müssen auf Layer 7 ausgerichtet sein und nicht nur Richtlinien und Zugriffsrechte auf Netzwerkebene regeln. Dadurch können Benutzer das Least-Privilege-Prinzip auf allen Ebenen (Layer 3 bis 7) berücksichtigen und detaillierte Zugriffsrichtlinien auf Anwendungsebene und untergeordneten Ebenen festlegen. So wird das Risiko minimiert, dass Benutzer zu umfangreiche Zugriffsrechte erhalten.

- Kontinuierliche verhaltensbasierte Überprüfung: Mit einem ZTNA 2.0-Modell wird auch nach der Gewährung des Zugriffs die Vertrauensbeziehung kontinuierlich überprüft. Dabei werden verschiedene Faktoren berücksichtigt, zum Beispiel die Benutzeraktivitäten, das Verhalten und der Unternehmenskontext. Werden verdächtige Aktivitäten erkannt oder eine Datenausschleusung befürchtet, kann der Zugriff auf eine App in Echtzeit widerrufen werden.

- Kontinuierliche Sicherheitsprüfung: Nachdem eine Verbindung hergestellt wurde, wird der gesamte Datenverkehr kontinuierlich überprüft, auch für zulässige Verbindungen. Auf diese Weise lassen sich alle Bedrohungen verhindern, einschließlich Zero-Day-Exploits. Das ist besonders wichtig, wenn die Anmeldedaten legitimer Benutzer gestohlen und für einen Angriff auf Anwendungen und Infrastrukturen ausgenutzt werden.

- Schutz für alle Daten: Mit einem ZTNA 2.0-Modell haben Unternehmen nun dank einer zentralen Managementkonsole und einer einheitlichen Richtlinie einen umfassenden Überblick und konsistente Kontrolle über sensible Daten in allen Anwendungen. Außerdem kann in dem neuen Modell auch DLP für alle Daten angewendet werden – in alten On-Premises-, öffentlichen Cloud- oder SaaS-Anwendungen.

- Umfassende Abdeckung von Anwendungen: Es werden alle Anwendungen (öffentliche, private/On-Premises- und Cloud-Anwendungen) und alle Datenzugriffsmodelle (remote und hybrid) unterstützt. So kann eine echte Zero-Trust-Architektur erstellt werden und nicht nur ein Modell für den Remotezugriff. ZTNA 2.0-Lösungen sollten mithilfe von tiefgreifenden und kontinuierlichen Sicherheitsprüfungen gewährleisten, dass der Datenverkehr geschützt ist. Dabei werden mithilfe maschineller Lernverfahren alle Bedrohungen erfasst und Zero-Day-Angriffe inline verhindert.

Neben diesen fünf Funktionen, die die Schwachstellen der ZTNA 1.0-Lösungen beheben, sollten Entscheidungsträger weitere Kriterien berücksichtigen, damit auch zukünftige Anforderungen an die Risikominimierung und das Wachstum bei hybriden Arbeitsmodellen erfüllt werden. Wird ZTNA in eine SASE-Plattform integriert, profitieren Unternehmen von einer einfachen, konsistenten Verwaltung, höheren Effizienz und konsistenten Durchsetzung von Richtlinien und Zugriffsregeln für alle Anwendungen und Benutzer in der Umgebung. Außerdem darf das Nutzererlebnis nicht beeinträchtigt werden. Aufgrund der zunehmenden Verbreitung hybrider Arbeitsmodelle sollte dafür gesorgt werden, dass Benutzer problemlos auf die benötigten Anwendungen zugreifen können, unabhängig von ihrem Standort und Arbeitsplatz.

Prisma Access von Palo Alto Networks: cloudbasierter ZTNA 2.0

Palo Alto Networks hat kürzlich Prisma Access ergänzt, um die Anforderungen bezüglich Remotezugriff und Zero-Trust-Strategien in hybriden Arbeitsumgebungen zu erfüllen. Diese Lösung wird in der Cloud bereitgestellt und bietet echten Zero-Trust-Netzwerkzugriff 2.0. Zu den wichtigsten Funktionen gehören:

- Integrierter Schutz aller Benutzer und Anwendungen und detaillierte Zugriffskontrollen für Benutzer und Anwendungen: Mit Prisma Access können Unternehmen das Least-Privilege-Prinzip von Layer 3 bis 7 durchgehend umsetzen und Kontrollen auf diversen Ebenen wie der Anwendungsebene und niedrigeren Ebenen und für App-Funktionen und App-Aktivitäten durchsetzen. Das gilt für alle Benutzer, Anwendungen und Standorte.

- Kontinuierliche verhaltensbasierte Überprüfung der Vertrauensbeziehung: Bei verdächtigem Verhalten oder vermuteter Datenausschleusung kann der Zugriff auf eine Anwendung in Echtzeit widerrufen werden, um Risiken und potenzielle Schäden zu minimieren. Diese kontinuierliche Überprüfung der Vertrauensbeziehungen ersetzt das „Zulassen-und-ignorieren“-Prinzip der ZTNA 1.0-Lösungen.

- Tiefgreifende und kontinuierliche Sicherheitsprüfung des Datenverkehrs: Prisma Access bietet eine Single-Pass-Prüfung des Datenverkehrs für alle Bedrohungsarten und damit eine hohe Leistung und geringe Latenz. Dank maschineller Lernverfahren können Bedrohungen inline abgewehrt werden, ganz ohne Signaturen. Da Prisma Access in eine Plattform integriert ist, sind auch andere Funktionen wie die Abwehr von Bedrohungen, Malwareanalysen, Advanced URL Filtering und DNS Security verfügbar.

- Konsistenter Schutz aller Anwendungen in allen Zugriffsmodellen: Prisma Access ZTNA 2.0 unterstützt alle Benutzer und Anwendungen im Unternehmen, das heißt Apps in On-Premises-, öffentlichen Cloud- und SaaS-Umgebungen sowie ältere und moderne/cloudnative Anwendungen. Benutzer können Verbindungen zu Prisma Access ZTNA 2.0 mit oder ohne Agenten herstellen und sind immer sicher und geschützt.

- Standortunabhängiger Schutz der Daten: Prisma Access schützt sowohl den Zugriff als auch die Daten selbst durch konsistente Kontrollmechanismen für alle Anwendungen im Unternehmen und eine einzige Richtlinie für den Schutz vor Datenverlust. Prisma Access ist eine cloudbasierte Lösung und wurde speziell für Cloud-Umgebungen konzipiert. Sie kann daher die Funktionen für flexible Skalierbarkeit und Verfügbarkeit der führenden Hyperscale-Cloud-Anbieter nutzen.

- Einheitliche Verwaltung und konsistentes Nutzererlebnis: Mit Prisma Access erhalten Unternehmen eine einheitliche Plattform, die Netzwerk- und Sicherheitsteams die Verwaltung und Bereitstellung vereinfacht und Benutzern eine hohe Leistung sowie ein konsistentes und stabiles Nutzererlebnis für alle Anwendungen, Geräte und Standorte bietet. Das Architekturmodell von Prisma Access ermöglicht eine Verfügbarkeit von 99,999 Prozent, Sicherheitsverarbeitungszeiten von 10 ms und ein Leistungs-SLA für SaaS-Anwendungen (Software-as-a-Service). Prisma Access umfasst zudem natives Autonomous Digital Experience Management (ADEM), sodass Probleme proaktiv identifiziert, isoliert und behoben werden können, bevor die Benutzer etwas davon bemerken.

Fazit

Der Druck auf Unternehmen, mobile und hybride Arbeitsplätze anzubieten, nimmt stetig zu. Anwendungen und Benutzer sind inzwischen nicht mehr standortgebunden, sodass die Unternehmensarchitektur direkte Verbindungen zu Anwendungen unterstützen muss, statt den gesamten Datenverkehr über Rechenzentren zu leiten. Diese Transformation hat allerdings weitreichende Auswirkungen auf die Sicherheitsstrategien von Unternehmen, insbesondere in Umgebungen, die vermehrt von komplexen Cyberbedrohungen und gezielten Kampagnen gegen Remotebenutzer angegriffen werden.

Mit Lösungen für den Zero-Trust-Netzwerkzugriff konnten Unternehmen vorübergehend die pandemiebedingten neuen Anforderungen erfüllen, aber die zunehmende Nachfrage nach Remotezugriff und hybriden Arbeitsmodellen hat Lücken in der Technologie aufgedeckt. Diese müssen geschlossen werden, damit Unternehmen die von ihren Mitarbeitern geforderten flexiblen, produktiven und sicheren hybriden Arbeitsplätze anbieten können.

Palo Alto Networks ist schon seit Jahren für seine innovativen Lösungen für Netzwerksicherheit, Endpunktsicherheit, Zero Trust und Remotezugriff bekannt. Wir haben nicht nur die Schwachstellen in den ZTNA 1.0-Lösungen aufgedeckt, sondern schließen diese Lücken auch mit ZTNA 2.0 in Prisma Access. Es ist die erste ZTNA-Lösung, die echte Zero-Trust-Funktionen bietet, zum Beispiel Least-Privilege-Zugriff, kontinuierliche verhaltensbasierte Prüfung der Vertrauensbeziehungen, tiefgreifende und kontinuierliche Sicherheitsprüfungen sowie konsistente Kontrolle der Daten für alle Anwendungen. Außerdem bietet Prisma Access dank einer einheitlichen Plattform und Verwaltungskonsole eine hohe Leistung und ein konsistentes Nutzererlebnis.

Enterprise Strategy Group ist ein Marktforschungsunternehmen, das integrierte Technologieanalysen und Studien durchführt, Strategien entwickelt und der globalen IT-Community aussagekräftige Erkenntnisse und Services für Go-to-Market-Inhalte bereitstellt.

www.esg-global.com contact@esg-global.com +1 508 482 0188