eBOOK

www.security-insider.de

SECURITY INSIDER

Zero Trust – das neue Normal der Security

Was Zero Trust wirklich bedeutet

Netzwerkzugang und Datensicherheit

Anwendung von Zero Trust in der Praxis

Powered by:

netskope

Inhalt

Vogel IT-Medien GmbH
Max-Josef-Metzger-Str. 21, 86157 Augsburg
Telefon +49 (0) 821/2177-0
E-Mail redaktion@security-insider.de
Web www.Security-Insider.de
Geschäftsführer: Werner Nieberle , Günter Schürger
Chefredakteur: Peter Schmitz, V.i.S.d.P., peter.schmitz@vogel.de
Erscheinungstermin: März 2022
Titel: Production Perig/stock.adobe.com

Was Zero Trust wirklich bedeutet

Mit zunehmendem Druck auf die IT durch neue Anforderungen wie Hybrid Work, die Digitalisierung der Geschäftsmodelle und die zunehmend verteilte Datenhaltung wird Zero Trust von vielen Entscheidungsträgern als die Lösung der Wahl zum Schutz ihrer Daten, Anwendungen und Systeme gesehen, so die EU-Agentur für Cybersicherheit ENISA. Doch was genau verbirgt sich hinter Zero Trust?


© tippapatt/AdobeStock

Business Asset wird, dessen Schutz extrem hohe Priorität besitzt und dessen Verlust kritisch für Unternehmen sein kann.

Auf den ersten Blick erscheint „Zero Trust" im Gegensatz zu „Trust" zu stehen, doch das genaue Gegenteil ist der Fall. Zero Trust erweist sich als Security-Grundlage dafür, Trust in der Digitalisierung erreichen und erhalten zu können.

Was unter Zero Trust verstanden wird

„Trust" gilt als neuer, zentraler Wert für Unternehmen in der digitalen Transformation. So sagt zum Beispiel IDC, Trust ist eine entscheidende Ressource, denn Vertrauen ist nicht nur Basis für Geschäfte, wenn es von Kunden entgegengebracht wird, sondern auch für Business-Ökosysteme und Innovationen mit Partnern. IDC ist fest davon überzeugt, dass Trust zu einem immer wichtigeren

Wörtlich kann man unter Zero Trust erst einmal verstehen: Traue niemandem, ganz gleich, wer es ist, wo er ist, und ob er sich innerhalb oder außerhalb des Firmennetzwerks befindet. Als Leitlinien von Zero Trust kann man sehen:

- Man darf keinem Nutzer, keinem Gerät und keiner Anwendung ein Anfangsvertrauen zugestehen.
- Das Vertrauen muss erarbeitet werden, man muss also die Vertrauenswürdigkeit überprüfen.

- Auf alle Ressourcen muss unabhängig vom Standort auf sichere Weise zugegriffen werden können.
- Die Zugangs- und Zugriffskontrolle muss auf der Basis von Need-to-know erfolgen und strikt durchgesetzt werden.
- Unternehmen müssen ihren Datenverkehr überprüfen und protokollieren, um sicherzustellen, dass die Nutzenden das Richtige tun.

Zugänge und Zugriffe werden also durchgehend hinsichtlich der Risiken, die dadurch entstehen, untersucht. Veränderungen in den Risiken werden dynamisch beantwortet. So kann ein bestehender Zugang zu einem Service unterbrochen, ein Nutzer und ein Gerät ausgesperrt werden.

Welche Modelle es für Zero Trust gibt

Das National Institute of Standards and Technology (NIST) beschreibt Zero Trust so: Zero Trust bezieht sich auf eine sich entwickelnde Reihe von Sicherheitsparadigmen, die die Verteidigung von großen Netzwerkperimetern auf einzelne oder kleine Gruppen von Ressourcen eingrenzen. Sein Fokus auf dem Schutz von Ressourcen statt auf Netzwerksegmenten ist eine Reaktion auf Unternehmenstrends, die Remote-Benutzer und Cloud-basierte Assets umfassen, die sich nicht innerhalb eines unternehmenseigenen Perimeters befinden.

Den Begriff Zero Trust hat das Analystenhaus Forrester Research geprägt. Von dort stammt auch das Modell „Zero Trust eXtended“. Dieses Modell sieht es als Erweiterung von Zero Trust an, wenn man bei der Risikobewertung zusätzlich folgende Aspekte betrachtet:

- das Netzwerk (Status Netzwerkisolation, Segmentierung und Sicherheit)
- die Daten (Kategorisierung von Daten, Isolation, Verschlüsselung und Kontrolle)
- die Mitarbeitenden (die von Nutzerinnen und Nutzern womöglich verursachten Bedrohungen)
- die Workloads (die Sicherheit der Clouds, Netzwerke, Apps)
- die Automatisierung und Orchestrierung (welche Systeme werden automatisch erkannt, klassifiziert und kontrolliert)
- die Sichtbarkeit der Systeme und Infrastrukturen („dunkle“ Ecken bei Systemen und Infrastrukturen erkennen)

Entsprechend erfordert Zero Trust:

- die Identifikation, Transparenz und Verwaltung bei Geräten, Apps und Diensten
- die Identifikation, Transparenz und Verwaltung bei Nutzenden
- jeweils ohne Unterscheidung zwischen internen und externen Nutzern, Netzwerken, Apps und Diensten
- jeweils an jedem Standort, ob On-Premises oder in der Cloud

Wie Zero Trust und die neue Art des Arbeitens zusammenhängen

Das eingangs genannte Zitat der EU-Agentur für Cybersicherheit ENISA macht deutlich, dass das Konzept Zero Trust mit zunehmender Digitalisierung immer wichtiger wird. Die Pandemie

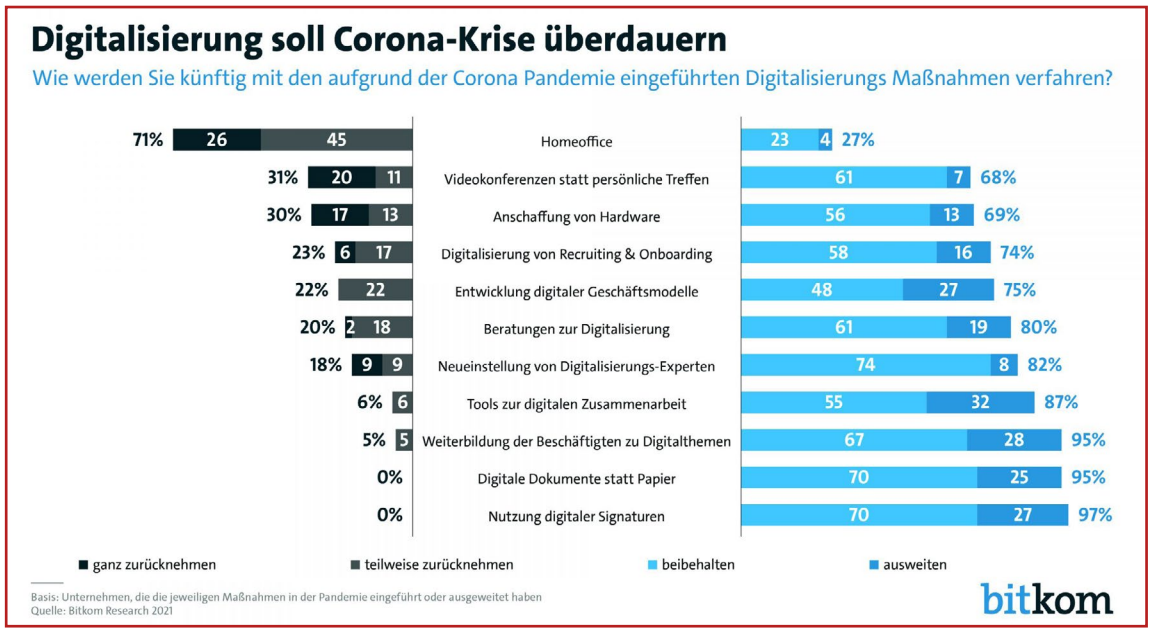
hat die Digitalisierung noch weiter beschleunigt und damit Zero Trust auf der Security-Agenda noch weiter nach vorne gebracht.

Zum einen mussten Prozesse und Dienste, die bislang noch nicht oder erst teilweise digitalisiert waren, so schnell wie möglich digital transformiert werden, um Gesellschaft, Wirtschaft und Staat auch in Zeiten einer Pandemie arbeitsfähig zu halten.

Zum anderen haben sich Arbeitsformen wie Homeoffice, mobile Arbeit und der flexible Wechsel zwischen Büro, Homeoffice und mobiler Arbeit, auch Hybrid Work genannt, weiter durchsetzen können, ja sie sind zeitweise zur Pflicht für Unternehmen geworden.

Damit hat sich einerseits die genutzte IT-Infrastruktur gewandelt. Cloud-Services, Cloud-Apps, mobile Endgeräte und mobile Apps spielen eine immer wichtigere Rolle in der IT-Nutzung. Gleichzeitig haben sich die Zugänge und Zugriffe auf Daten und Applikationen verändert. Zugänge und Zugriffe erfolgen nicht mehr vornehmlich innerhalb des Unternehmensnetzwerkes, sondern sie erfolgen über das Internet, indem zum Beispiel mobile Endpoints über das Internet auf Cloud-Services zugreifen.

Die flexible und standortunabhängige Nutzung der IT hat dazu geführt, dass das Internet nun das „neue Unternehmensnetzwerk" geworden ist. Damit muss sich aber auch die Sicherheit des Netzwerkes verändern. Sie kann nicht mehr durch Netzwerksicherheitskomponenten gewährleistet werden, sie muss genau wie die Services aus der



Der durch die Corona-Pandemie in der deutschen Wirtschaft ausgelöste Digitalisierungsschub ist von Dauer, so eine Umfrage des Digitalverbands Bitkom. Eingeleitete Maßnahmen wie Videokonferenzen oder Kollaborationstools, aber auch die Entwicklung neuer digitaler Geschäftsmodelle werden mehrheitlich beibehalten oder sogar noch ausgeweitet. Entwicklungen wie Hybrid Work müssen in den Security-Modellen dauerhaft berücksichtigt werden. Hier kommt Zero Trust zum Tragen. (Bild: Bitkom)

Cloud stammen, damit sie standortübergreifend die Zugänge und Zugriffe überwachen und regeln kann.
Genau das leistet Zero Trust aus der Cloud.

Warum die Sicht auf Zero Trust erweitert werden muss

Es zeigt sich zudem, dass eine Idee von Zero Trust, die nur die Nutzenden und die Geräte in den Blick nimmt, deutlich zu eng gedacht ist. Wie das zuvor erwähnte erweiterte Zero-Trust-Modell darstellt, erfordert die neue hybride IT-Nutzung auch ein neues umfassenderes Bild von Zero Trust.
Neben Anwenderinnen und Anwendern sowie Geräten muss Zero Trust auch alle IT-Ressourcen umfassen, die außerhalb des klassischen Unternehmensnetzwerkes genutzt werden, also auch Cloud-Services, Cloud-Apps sowie private Geräte, die von den Beschäftigten betrieblich genutzt werden (BYOD, Bring Your Own Device). Ein Trend, der mit den steigenden Arbeitsplatzzahlen in Homeoffices ebenfalls deutlich angewachsen ist.
Zero Trust ist damit die Sicherheit im neuen Normal. *Oliver Schonschek*

Zero Trust Network Access ist nicht alles

Wenn es um Zero Trust geht, hört und liest man oft von ZTNA (Zero Trust Network Access). Doch ZTNA ist nur eine Facette von Zero Trust. Das wird schnell deutlich, wenn man sich klarmacht, dass es nicht immer ausreichen wird, den Zugang zu einem Netzwerk abzusichern. Es muss auch um die Daten und ihre Sicherheit gehen, innerhalb und außerhalb des Netzwerks.

© momius/AdobeStock

Das ist ZTNA

Das Ziel von Zero Trust ist es, alle erforderlichen Ressourcen wie Applikationen, Daten und Netzwerke standortübergreifend verfügbar zu machen und die Risiken von Cyberattacken auf die Ressourcen zu minimieren. Dazu kommen bei Zero Trust zwei Sicherheitsansätze zum Einsatz: „Zero Trust Network Access" (ZTNA) und „Zero Trust Data Protection" (ZTDP).

Wer sich mit Zero Trust bereits befasst hat, wird in der Regel bereits auf den Begriff ZTNA gestoßen sein. Wie erwähnt, ist dies nur eine Facette von Zero Trust, die aber besonders im Fokus steht, wenn neue Sicherheitsansätze gesucht werden, um Fernzugriffe bei Remote Work besser abzusichern.

ZTNA ist ein Cloud-basierter Ansatz für den sicheren Netzwerkzugang und ersetzt die bisher häufig genutzten VPN-Funktionen (Virtual Private Network). ZTNA sorgt dafür, dass das Internet für einen sicheren Zugang genutzt werden kann, ob es Zugriffe auf On-Premises-Applikationen oder auf Cloud-Dienste sind.

Dazu bietet ZTNA insbesondere Funktionen wie sicherer Fernzugriff, starke

Benutzerauthentifizierung und eine Regelung und Überwachung der Zugriffsberechtigungen.

Darum ist Zero Trust Data Protection wichtig

Neben ZTNA spielt bei Zero Trust aber auch Zero Trust Data Protection (ZTDP) eine zentrale Rolle, die nicht übersehen werden darf. ZTDP stellt nicht die Zugriffe, sondern die Daten selbst in den Mittelpunkt. Die Daten werden dadurch an jedem Standort gegen unberechtigte Nutzung geschützt, gegen unerlaubten Datenabfluss, gegen Datenausspähung und Datenmanipulation.

Die Unternehmen in Deutschland reagieren auf die angespannte IT-Sicherheitslage und investieren mehr in Cyber-Security. Zu den Treibern der Security gehören Cloud Computing, mobiles Arbeiten und Homeoffice, so ein Ergebnis der IT-Sicherheitsumfrage 2022 des eco – Verbands der Internetwirtschaft e. V. Die veränderte Bedrohungslage und die neue Art der IT-Nutzung müssen eine Antwort finden in der Security. (Bild: eco)

ZTDP sorgt darüber hinaus für eine fortlaufende Risikobewertung, berücksichtigt bei der Sicherung des Datenzugriffs den Datenkontext und hilft so, die so wichtigen Compliance-Vorgaben einzuhalten, wie zum Beispiel den Datenschutz.

Das versteht man unter SASE

In Verbindung mit Zero Trust trifft man auch auf Konzepte wie „Secure Access Service Edge“ (SASE). Es ist wichtig, genau zu verstehen, was SASE mit Zero Trust zu tun hat.

SASE steht für Cloud-basierte Sicherheit und Cloud-basierte Netzwerkdienste und dient dem Schutz der Daten und Applikationen. Die Cloud-Basis ist entscheidend, denn durch die hybride, standortunabhängige IT-Nutzung können Sicherheit und Networking-Dienste nicht mehr durch die klassischen Netzwerk- und Security-Appliances bereitgestellt werden, sie müssen aus der Cloud kommen.

SASE übernimmt dabei die Aufgaben der bisherigen Netzwerk- und Security-Appliances, bietet sie als Cloud-Services an und vereint Funktionen in sich, die bisher getrennt von Firewalls, Secure Web Gateways (SWG), Lösungen für Data Loss Prevention (DLP) und CASB (Cloud Access Security Brokers) bereit gestellt wurden.

SASE ist in der Lage, Benutzer und Geräte zu identifizieren, richtlinienbasierte Sicherheitskontrollen anzuwenden und sicheren Zugriff auf die Anwendungen oder Daten bereitzustellen. SASE ermöglicht dadurch einen sicheren Zugriff unabhängig davon, wo sich Benutzer,

Daten, Anwendungen oder Geräte befinden – und genau das ist das Ziel eines Zero-Trust-Ansatzes.

Unterschied zwischen SASE und Security Service Edge (SSE)

Neben SASE gibt es eine weitere Abkürzung, die man kennen sollte, wenn es um die Umsetzung von Zero Trust geht: „Security Service Edge" (SSE). Vereinfacht gesagt, könnte man SSE als die Security im SASE-Konzept bezeichnen. SSE bietet damit insbesondere die Funktionen von Firewalls, Cloud Access Security Broker (CASB), Secure Web Gateway (SWG) und Zero Trust Network Access (ZTNA).

Wesentlich für SSE ist, dass Sicherheit überall dort sein muss, wo die Daten sind. Die Sicherheit muss in der Lage sein, den Cloud-Datenverkehr zu überwachen und zu analysieren. Die Sicherheit muss bei der Risikobewertung immer den Kontext der Daten berücksichtigen. Nicht zuletzt darf es nicht dazu kommen, dass die Sicherheit das Netzwerk belastet, die Performance also unter der Security leidet.

Wie alles zusammenhängt

Wenn man nun SASE, SSE und Zero Trust im Blick hat, werden auch die Zusammenhänge klar, die wichtig sind, um entsprechende Lösungen auf dem Markt richtig einschätzen zu können.

SSE bietet Cloud-basierte Sicherheitsdienste als Teil einer SASE-Architektur. SSE-Lösungen integrieren Zero-Trust-Prinzipien als grundlegende Sicherheit in ihre Architektur. Alles, von der Datenbewegung bis zum Netzwerkzugriff, unterliegt Zero Trust, jeder Benutzer, jede Benutzerin wird authentifiziert, man erhält nur Zugriff auf genau das, was wirklich benötigt wird, jeweils unter Berücksichtigung des aktuellen Kontextes und Risikos. *Oliver Schonschek*

Anwendung von Zero Trust in der Praxis

Über Zero Trust wird meistens dann gesprochen, wenn es um Remote Work und die Absicherung von Fernzugriffen der Beschäftigten auf das Unternehmensnetzwerk geht. Doch Zero Trust ist weitaus mehr und kann deutlich mehr. Das zeigen die vielfältigen Anwendungsfälle von Zero Trust in der Praxis.


© Prostock-studio/AdobeStock

Alle Möglichkeiten von Zero Trust nutzen

Zero Trust Network Access (ZTNA) kann mehr, als bestehende VPN-Verbindungen von Homeoffices mit dem Unternehmensnetzwerk zu ersetzen. Dies ist nur ein Anwendungsfall, wenn auch ein sehr wichtiger in Zeiten von Hybrid Work als Mischform von Büroarbeit, Tätigkeit im Homeoffice und mobiler Arbeit.

Betrachtet man Zero Trust übergreifend, kann man sagen: Zero Trust ermöglicht den sicheren Zugriff auf private Applikationen, auf Basis einer Risikobewertung und Kontrolle der digitalen Identitäten der Anwenderinnen und Anwender und der genutzten Geräte. ZTNA ermöglicht aber auch eine sichere und direkte Verbindung zu Diensten in Public Clouds, ohne den Umweg über die Unternehmensinfrastruktur. Dabei werden die Applikationen und die Daten in Public Clouds und Private Clouds vor Attacken und unbefugten Zugriffen geschützt. Nicht zuletzt wird die IT-Nutzung entscheidend vereinfacht, denn die Zugriffe auf private Anwendungen und Cloud-Apps werden vereinheitlicht.

Diese Vorteile kann Zero Trust in vielen verschiedenen Anwendungsfällen ausspielen, von denen einige hier näher betrachtet werden sollen.

Anwendungsfall Remote Work

Zuerst sei der bereits erwähnte Fall von Remote Work genannt. Dieser Anwendungsfall ist meistens der Einstieg eines

Unternehmens in den Bereich Zero Trust. Man sollte aber nicht dabei stehen bleiben, dass sich dank ZTNA die Beschäftigten sicher mit Unternehmensnetzwerken und Anwendungen verbinden können.

ZTNA überwindet die Nachteile, die traditionelles VPN mit sich bringen kann. Die Nutzenden erhalten nicht einfach Zugang zu allem, was über ein VPN zu erreichen ist, sondern zuerst werden die Risiken des Zugriffs, die vorhandenen Berechtigungen und der tatsächliche Bedarf überprüft. Was nicht im Zugriff sein muss, ist es auch nicht, ein klarer Sicherheitsvorteil bei Remote Work und bei jedem Zugriff auf Unternehmensressourcen und Cloud-Ressourcen.

Anwendungsfall BYOD

Neben Remote Work ist auch Bring Your Own Device (BYOD) zunehmend wichtig für Unternehmen geworden. Geräte, die nicht zum Unternehmen gehören, können auf Basis von Zero Trust Zugriff erhalten, nach einer Sicherheitskontrolle und auf Basis der Risikobewertung.

Das gilt aber nicht nur für Beschäftigte, die private Geräte betrieblich nutzen. Auch Geschäftspartner und andere Dritte, die temporär bestimmte Zugriffsrechte erhalten sollen, können über Zero Trust sicher eingebunden werden. Externe Geräte und externe Identitäten können so in die Sicherheitsarchitektur einbezogen werden.

Anwendungsfall Migration in die Cloud

Da ZTNA sowohl die Zugriffe auf private Applikationen des Unternehmens als auch die Zugriffe auf Cloud-Applikationen absichert, ist Zero Trust der Ansatz der Wahl für die Migration in die Cloud. Die Zugriffe auf alle genutzten IT-Ressourcen sind einheitlich möglich – in der Cloud und im Unternehmensnetzwerk. Cloud-Ressourcen sind über ZTNA direkt zugänglich, Umwege über Unternehmensinfrastrukturen werden vermieden, wichtig für möglichst gute Performance und möglichst wenig Komplexität bei den Verbindungen.

Anwendungsfall DevOps

Als weiteres, konkretes Beispiel für die Vorteile von Zero Trust soll DevOps genannt werden, die Verbindung und Verzahnung von Development und Operations. Die Entwicklerinnen und Entwickler arbeiten dabei zunehmend Cloud-basiert und standortunabhängig.

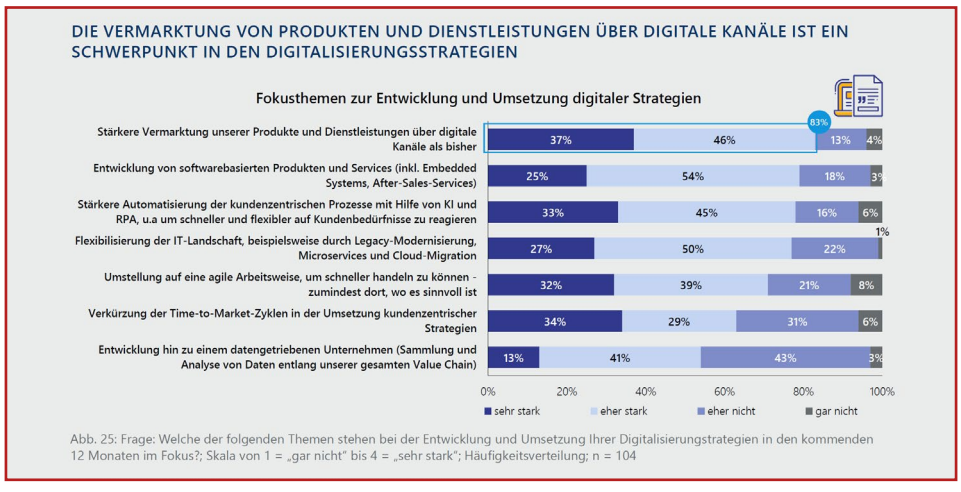


Abb. 25: Frage: Welche der folgenden Themen stehen bei der Entwicklung und Umsetzung Ihrer Digitalisierungstrategien in den kommenden 12 Monaten im Fokus?; Skala von 1 = „gar nicht" bis 4 = „sehr stark"; Häufigkeitsverteilung; n = 104

Bei der digitalen Transformation haben Unternehmen zahlreiche Fokusthemen. Die Flexibilisierung der IT-Landschaft zum Beispiel erfordert auch eine Transformation der Security, wie sie durch Zero Trust ermöglicht wird. (Bild: Lünendonk-Studie „Der Markt für Digital Experience Services in Deutschland", Lünendonk & Hossenfelder)

Mit ZTNA können sie Ressourcen, die sie benötigen und auf die sie zugreifen dürfen, sicher erreichen, ob sich diese nun im Rechenzentrum oder in einer Cloud befinden. DevOps kann so ohne Umwege und Verzögerungen realisiert werden.

Zero Trust für die Transformation der Security

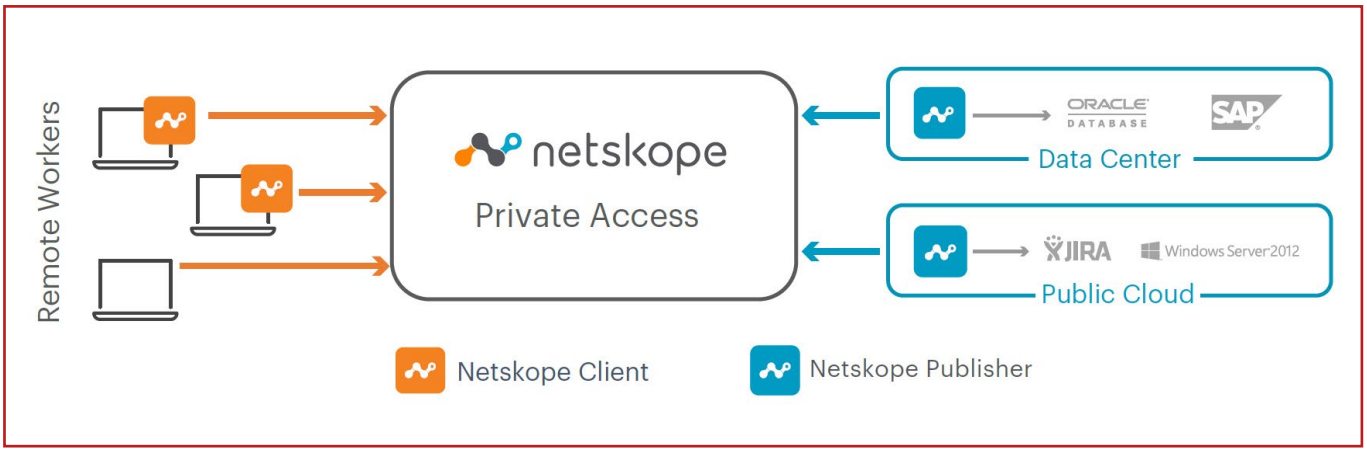
Betrachtet man die Beispiele, wird deutlich, wie sehr Zero Trust zu der fortschreitenden digitalen Transformation passt. Tatsächlich muss sich die Security transformieren, um die digitale Transformation absichern zu können.

Die Transformation der Security wird möglich durch Zero Trust, indem Daten und Applikationen gegen Attacken und unbefugte Zugriffe geschützt werden – On-Premises und in der Cloud. Die Nutzung des Internets, die zu einer vergrößerten Angriffsfläche geführt hat, wird gesichert ermöglicht, da die Nutzung des Internets und des klassischen Unternehmensnetzwerks mit den gleichen Sicherheitsmaßnahmen geschützt werden. Überall gilt Zero Trust. Das transformiert die Security für die hybride IT-Nutzung und für Hybrid Work.

Oliver Schonschek

ZTNA als Teil eines Ökosystems

Zu einem Zero Trust-Konzept gehören eine einheitliche Oberfläche zur Administration und Konfiguration sowie eine native und offene Integration in das umliegende Ökosystem.



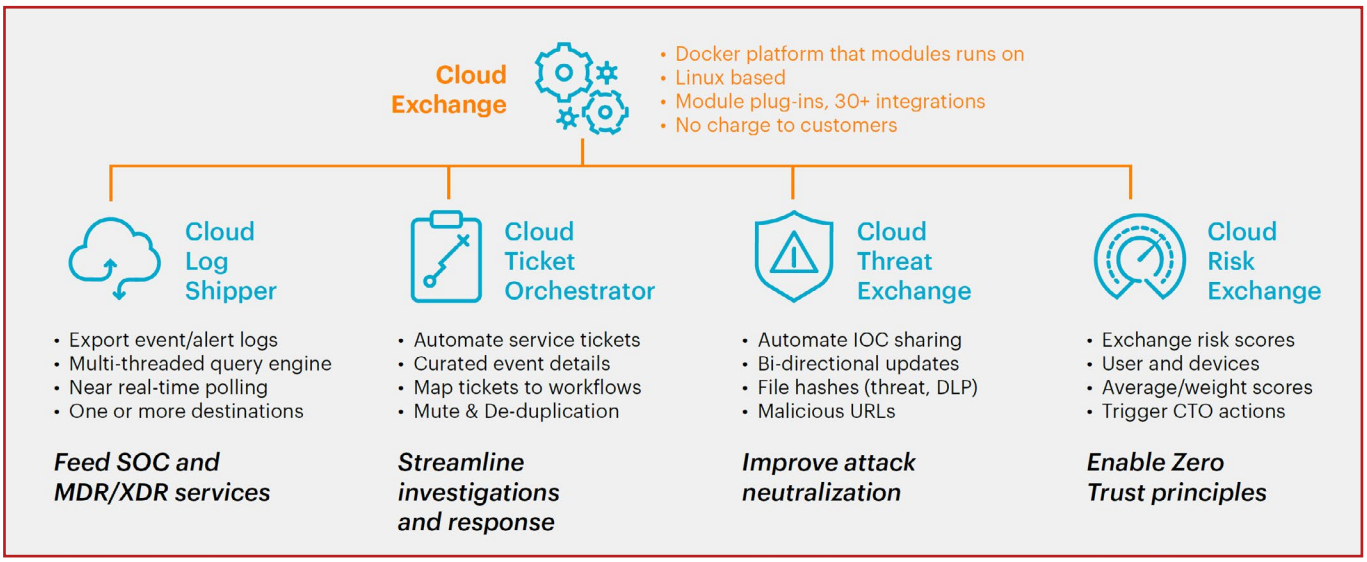
Netskope Private Access, als Teil einer Zero Trust Network Access-Architektur, erlaubt es Unternehmen nicht nur Zugriffe von Anwendern und Geräten auf Web, Cloud-Anwendungen und Cloud-Infrastruktur abzusichern – auch Zugriffe auf private Anwendungen können so zentralisiert verwaltet werden. Entscheidend sind dabei eine einheitliche Oberfläche zur Administration und Konfiguration sowie eine nahtlose Integration in die vorhandene Infrastruktur.

Wie bereits erwähnt umfasst eine SASE/SSE-Architektur nicht ausschließlich ZTNA, es sollte daher nahtlos in das Policy Framework anderer SSE-Komponenten (Web Proxy, CASB, DLP, CSPM, SSPM) mit eingebunden werden. Dies ermöglicht eine zentralisierte Verwaltung der Zugriffe auf Anwendungen und Ressourcen aller Art.

Ein weiterer Aspekt eines Zero Trust-Konzeptes ist – und das sollte nicht außer Acht gelassen werden – eine native und offene Integration in das umliegende Ökosystem. Dies besteht auf diversen Komponenten wie beispielsweise Endpoint Detection & Remediation (EDR), Identity Access Management (IAM), Security Information and Event Management (SIEM) und vielem mehr.

Dies zeigt auf, dass ein Zero Trust-Ansatz oftmals ein geschlossener Kreislauf ist, sodass alle Netzwerk- und Sicherheitskomponenten Daten miteinander austauschen können, welche dann wiederum durch Netzwerk- und

Netskope Zero Trust Network Access



Security-Kontext zu verwertbaren und umsetzbaren Informationen werden. So können durch Netskopes Cloud Exchange-Lösung beispielsweise Indicators of Compromise (IOCs) gegenseitig mit anderen Systemen ausgetauscht werden, Service Tickets automatisiert erstellt werden, Anwender-Risk-Ratings an IDP-Systeme übermittelt werden, Logs und Events in Echtzeit übertragen werden und vieles mehr.

Sie merken, Zero Trust Network Access ist Teil eines Ökosystems. Ein Ökosystem, welches von Netskope als Marktführer im Bereich Security Service Edge assimiliert wurde und kontinuierlich auf einer cloud-nativen, skalierbaren Plattform aus der Cloud – für die Cloud – weiterentwickelt wird.

Phil Rumi, Senior Sales Engineer CEUR, Netskope