Whitepaper

Zero Trust Network Access: Die Umstellung lohnt sich — für die IT und fürs Unternehmen

Digitale Unternehmenstransfor-mation ohne Abstriche in puncto Datenschutz

Technologie ist heute mehr als nur ein Motor für das Geschäftswachstum: Zunehmend setzt sich die Erkenntnis durch, dass sie als eigenständiger Erfolgsfaktor neue Umsatzchancen und Effizienzgewinne ermöglicht. Mit der zunehmenden Bedeutung von Technologie-Initiativen hat auch die Rolle der IT-Beauftragten eine Aufwertung erfahren, sodass CISOs, CIOs und CTOs mittlerweile bei vielen Unternehmen in der Geschäftsführung sitzen.

Hauptursächlich bedingt wurde diese Entwicklung zum einen durch den rapiden Umstieg auf Cloud-basierte Infrastrukturen wie Azure, AWS und Google Cloud, zum anderen durch die zunehmende Nutzung privater Mobilgeräte zum Zugriff auf Geschäftsanwendungen im Rahmen sogenannter BYOD-Modelle. Unternehmen profitieren dadurch von handfesten Vorteilen in Bezug auf die Optimierung von Geschäftsprozessen und die Möglichkeit, Produkte und Dienstleistungen schneller und mit geringerem Kostenaufwand bereitzustellen.

Mit der Einführung dieser Technologien gehen jedoch auch beträchtliche Risiken einher.

Der Umstieg von herkömmlichen Unternehmensnetzwerken auf Cloud-Umgebungen und User-Mobilität hat zum Verschwinden des Sicherheitsperimeters geführt, der User und interne Services bisher zuverlässig schützte.

Entsprechend sind IT-Verantwortliche beim Beantragen des Budgets für Neuanschaffungen zur Unterstützung der Verlagerung zur Cloud sowie der zunehmenden Mobilität gefordert, gegenüber der Geschäftsführung den Zusammenhang zwischen Cyberrisiken und potenziellen Geschäftsfolgen klipp und klar zu kommunizieren. Insbesondere ist dabei auf die Kosten von Datenpannen, Ausfallzeiten in geschäftskritischen Infrastrukturen und Schädigungen des Markenrufs hinzuweisen. Mit anderen Worten: IT-Verantwortlichen muss es gelingen, die Geschäftsführung mit betriebswirtschaftlichen Argumenten von der Notwendigkeit der beantragten Anschaffungen zu überzeugen.

Dabei empfiehlt es sich, zunächst basierend auf einer Analyse des Risikoportfolios die Risikoaversion des Unternehmens zu berechnen. Möglicherweise sind geschäftskritische Anwendungen mit SOC-1 oder ISO 27001 konform und erfordern zusätzliche Sicherheitsschichten. Diese sind der geschäftskritischen Infrastruktur zuzurechnen. Unter Umständen muss eine isolierte Umgebung für Transaktionen mit bestimmten Ländern (z. B. China) eingerichtet werden. Bei Legacy-Infrastrukturen ist eine laufende Überprüfung auf eventuell notwendige Patches erforderlich, denn schon eine einzige fehlende Firewall-Konfiguration kann dem Unternehmen massive Probleme bereiten.

Herausforderungen beim Umstieg auf Cloud und Mobilität

Unterm Strich kommt es darauf an, geschäftskritische Initiativen zu unterstützen und die Lücke zwischen Geschäftsanforderungen und aktuellen IT-Kapazitäten zu schließen. Bei Kaufentscheidungen sollten daher folgende Kriterien maßgebliche Beachtung finden:

1. Inwieweit trägt die betreffende Lösung zur effizienten Abwicklung anfallender Aufgaben sowie zur Entlastung der Mitarbeiter bei?
2. Gewährleistet sie eine hervorragende User Experience für interne und externe Anwender?
3. Trägt sie zur Minderung von Risiken bei, die die Produktivität, den Schutz geistigen Eigentums und den Markenruf gefährden?
4. Ist sie anpassungsfähig und agil genug, um eine dynamische Geschäftsentwicklung mittragen und unterstützen zu können?
5. Ermöglicht sie eine beschleunigte digitale Transformation durch Wechsel in öffentliche Cloud-Umgebungen?

Bei jeder Kaufentscheidung wollen die Vor- und Nachteile der verschiedenen verfügbaren Lösungen sorgfältig gegeneinander abgewogen werden. So trägt etwa die Umstellung auf Cloud-Services und Mobilanwendungen zur Optimierung der User Experience bei. Andererseits wird dadurch die Minderung des Risikos von Cyberangriffen erschwert. IT-Verantwortliche müssen darauf achten, dass die beschleunigte Einführung neuer Technologien nicht auf Kosten der Sicherheit vertraulicher Daten geht. Entscheidend ist bei Neuanschaffungen sowohl die Auswahl der richtigen Technologie als auch das Timing der Umstellung.

Geschäftsnutzen von ZTNA-Services

Gartner empfiehlt IT-Verantwortlichen die Umstellung auf ZTNA im Rahmen einer SSE-Strategie (Security Service Edge) zur Gewährleistung flexibler und sicherer Konnektivität für hybride Belegschaften. ZTNA-Services unterstützen sicheren Zugriff auf interne Anwendungen für User an Remote-Standorten und in der Unternehmenszentrale ohne herkömmliche VPN-Technologien.

ZTNA-Services richten eine identitäts- und kontextbasierte, durch technische Zugriffskontrollen gesicherte Schutzgrenze um eine einzelne bzw. mehrere Anwendungen ein. Die Anwendungen sind nicht öffentlich sichtbar und der Zugriff darauf wird über einen Trustbroker auf eine festgelegte Gruppe namentlich definierter Entitäten beschränkt. Der Broker verifiziert User-Identität, Kontext und Richtlinientreue der jeweiligen Teilnehmer, bevor die Verbindung vermittelt wird. Damit werden unternehmenseigene Anwendungen im Internet unsichtbar gemacht, sodass sich die Angriffsfläche erheblich verkleinert.

Gartner

Schätzungen zufolge werden bereits 2025 mindestens 70 % aller neuen Remotezugriff-Bereitstellungen überwiegend über ZTNA (statt über VPN-Services) abgewickelt.

Aus Sicht des IT-Verantwortlichen trägt die Umstellung auf eine ZTNA-Lösung zur Realisierung der fünf bereits genannten Prioritäten bei:

1. Höhere Produktivität:

Im Zuge der pandemiebedingten „Great Resignation" haben bereits Millionen US-amerikanischer Arbeitnehmer ihre Festanstellung gekündigt. **Prognosen zufolge** wird der Trend auch in diesem Jahr ungebrochen anhalten. Unternehmen stehen damit der Problematik gegenüber, auf einem ohnehin schon angespannten Arbeitsmarkt qualifizierte Fachkräfte anwerben und dauerhaft binden zu müssen. IT-Verantwortliche können hier einen substanziellen Beitrag zum Geschäftserfolg leisten, indem einerseits die akuten Engpässe mittels geeigneter Technologien überbrückt und andererseits die Grundlagen für zukunftsfähige Arbeitskonzepte geschaffen werden. ZTNA empfiehlt sich als ausgesprochen benutzerfreundliche Lösung, die Usern u. a. die Mühe erspart, bei jeder Anmeldung im Netzwerk einen VPN-Client zu starten. Dadurch wird hohe Produktivität bei minimalem Frustfaktor gewährleistet. Die IT profitiert ebenfalls von einer Cloud-basierten Lösung ohne Hardware-Installationen, die sich einfach einrichten und bereitstellen lässt. Mit ZTNA wird eine sichere Umstellung auf Cloud-basierte Anwendungen möglich, die wiederum die Produktivität des IT-Teams und der gesamten Organisation steigert.

2. Optimierte User Experience:

User wollen heute von wechselnden Standorten aus auf Unternehmensanwendungen zugreifen: im Büro, im Homeoffice oder auch unterwegs. Erschwerend kommt hinzu, dass es sich bei diesen Usern teils um Mitarbeiter, teils um externe Dritte handelt. Gemeinsam ist ihnen der Anspruch, unabhängig vom Gerät, Standort oder Netzwerk reibungslosen Zugriff auf die jeweils benötigten Anwendungen zu erhalten. Mit ZTNA lässt sich sicherstellen, dass diese Erwartungen erfüllt und alle User zügig und nahtlos verbunden werden — ganz ohne VPN und lästige Anmeldungen. Für externe User und nicht verwaltete Geräte entfällt zudem die Installation eines Agents auf dem Endgerät.

Über die Optimierung der User Experience hinaus trägt der Einsatz eines clientlosen ZTNA-Service auch zur Steigerung der Produktivität bei, da Usern unabhängig vom Gerät und Standort richtlinienbasierter Zugriff auf unternehmenseigene Anwendungen gewährt wird.

3. Weniger Risiko:

Die Gewährleistung der Sicherheit erweist sich bei der Umstellung auf Cloud-Umgebungen und dezentrale Arbeitskonzepte weiterhin als Herausforderung. Ohne entsprechende Maßnahmen zum Schutz von Usern und Unternehmensressourcen besteht ein erhöhtes Risiko von Angriffen auf geschäftskritische Anwendungen und die Infrastruktur. Herkömmliche, netzwerkzentrierte Technologien wie VPNs und Firewalls bieten keinen ausreichenden Schutz. Remote-User werden automatisch als vertrauenswürdig eingestuft und direkt im Netzwerk platziert. Die erforderlichen Ereignisbehandlungsroutinen für eingehende Remote-Verbindungen prädestinieren VPNs geradezu als Trojanische Pferde, über die Ransomware ins Netzwerk geschmuggelt wird. Zudem erhalten sowohl lokale als auch Remote-User lateralen Zugriff auf sämtliche Ressourcen innerhalb des Netzwerks. Dies gilt für Mitarbeiter des Unternehmens ebenso wie für externe Dritte, die möglicherweise weniger stringente Sicherheitsmaßnahmen anwenden. ZTNA-Services verbinden ausschließlich befugte User (nach Prüfung ihrer Identität und des Sicherheitsstatus ihres Geräts) unter Anwendung Zero-Trust-basierter Richtlinien mit den jeweils angefragten unternehmenseigenen Anwendungen, die entweder in einer öffentlichen oder privaten Cloud oder im Rechenzentrum ausgeführt werden. Während ZTNA-Services ursprünglich primär zur Gewährleistung der Konnektivität eingesetzt wurden, werden sie inzwischen als vollständig integrierte Sicherheitslösungen bereitgestellt. Sie bieten wirksamen Schutz insbesondere vor Insider-Bedrohungen und Advanced Threats und tragen somit zur Verbesserung des Sicherheitsstatus insgesamt bei.

4. Cloud-basierte Agilität und Skalierbarkeit:

In vielen Organisationen nimmt mit der Anzahl der Mitarbeiter, User-Geräte und Anwendungen auch das Traffic-Volumen stetig zu. Da Cloud-basierte ZTNA-Services vom Anbieter gehostet werden, stellt die Hochskalierung der Kapazitäten keine zusätzliche Belastung für das IT-Team dar. Bei steigender Nachfrage werden die Kapazitäten des ZTNA-Service automatisch angepasst. Ebenfalls entfällt der Einsatz weiterer Hardware-Appliances oder virtualisierter Firewalls, der den Umstieg auf öffentliche Cloud-Umgebungen verlangsamen würde. Agilität und Skalierbarkeit sind maßgebliche Kriterien, an denen sich der Erfolg von Entscheidungsträgern im IT-Bereich misst. Mit ZTNA ist ihre Erfüllung gewährleistet.

5. Beschleunigte digitale Transformation:

Die Umstellung auf Cloud und Mobilität hat für viele Unternehmen hohe Priorität. Wenn diese Umstellung jedoch nicht durch geeignete Sicherheitslösungen unterstützt wird, können Monate oder gar Jahre vergehen, bevor es gelingt, das Potenzial der Cloud für eine globale User-Community aus Mitarbeitern und externen Dritten voll nutzbar zu machen. Nicht zuletzt ist dafür der hohe Verwaltungsaufwand bzw. Komplexitätsgrad verantwortlich, der entsteht, wenn nicht verwaltete User-Geräte über herkömmliche Netzwerk- und Sicherheitslösungen mit Cloud-basierten Anwendungen verbunden werden. ZTNA empfiehlt sich hier als weniger komplexe softwarebasierte Alternative, deren Implementierung nur Stunden — und nicht mehrere Monate oder gar Jahre — dauert. Entsprechend schneller zahlen sich auch die Investitionen in Cloud und Mobilität aus.

> „Ich bin zuversichtlich, dass wir mit den Änderungen, die wir im Zuge des Wechsels in die Cloud vorgenommen haben, hervorragend aufgestellt sind, um zukünftige Herausforderungen zu bewältigen. Diese Erfahrung wird dauerhafte Auswirkungen haben und eingeschliffene Denkmuster ein für allemal umstoßen. Wir öffnen den Kollegen und Kolleginnen die Augen für neue Arbeitsmethoden und erbringen zugleich einen überzeugenden Nachweis sowohl für den positiven Beitrag, den Technologie leisten kann, als auch die Resilienz und Kreativität unserer Belegschaft."
>
> — **Alex Philips,** Chief Information Officer, National Oilwell & Varco

Weitere Informationen über ZTNA

ZTNA-Services (Zero Trust Network Access) geben IT-Verantwortlichen in Unternehmen ein wertvolles Tool an die Hand. Zscaler Private Access (ZPA) ist der von Zscaler entwickelte ZTNA-Service und gewährleistet reibungslosen, sicheren Zugriff auf interne Anwendungen über unsere globale Cloud. Allzu oft wird die IT tendenziell als Kostenstelle angesehen. Mit einem erstklassigen ZTNA-Service kann sie ihren tatsächlichen Wert für das Unternehmen unter Beweis stellen.

Carlos Cong, Senior Manager für Enterprise Technology Services bei Paychex, berichtet über die Implementierung von ZTNA zur Vereinfachung und Beschleunigung der IT-Integrationen infolge von Fusionen und Übernahmen.

Zur Fallstudie von CMA-CGN

Zscaler bietet Unternehmen die Chance, die ZTNA-Lösung 7 Tage lang kostenlos zu testen.

7-tägige ZTNA-Demo starten

Für weitere Fragen sind unsere ZTNA-Experten jederzeit unter **sales@zscaler.com erreichbar.**

zscaler™ | Experience your world, secured.™

Über Zscaler
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Benutzern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust.
Die SASE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf **zscaler.de** oder folgen Sie uns auf Twitter **@zscaler**.

+1 408 533 0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA zscaler.de