Blueprint für die Rückkehr ins Büro: So bringt Zero Trust frischen Wind in Ihren Arbeitsplatz

WHITEPAPER

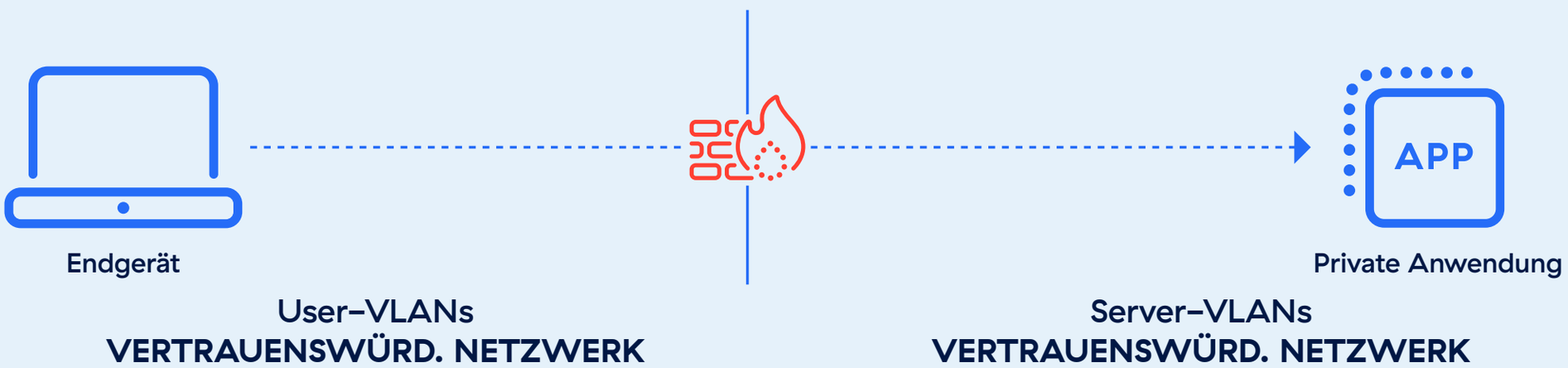
Die Rückkehr ins Büro bedeutet keinen Schritt zurück in die Vergangenheit. Die Mitarbeiter kommen zwar zurück an ihren Arbeitsplatz — Anwendungen und Daten jedoch nicht. Durch die jahrelange Remote- und Hybridarbeit sind Mitarbeiter mit Cloud-Anwendungen vertraut und nutzen sie regelmäßig. Mitarbeiter, die zurück ins Büro kommen, erwarten die gleiche — wenn nicht sogar höhere — IT-Zuverlässigkeit und -Performance. Die Rückkehr zu althergebrachten Methoden genügt nicht, um diese Erwartungen zu erfüllen.

Mit der Migration von Anwendungen und Daten in die Cloud muss überdacht werden, wie On-Premise-Sicherheit bereitgestellt werden kann, ohne die Produktivität zu beeinträchtigen. Ursprünglich zur Absicherung von Remote-Arbeit implementiert, liefert Zero Trust auch On-Premise dieselben Sicherheits- und Produktivitätsvorteile und ist ein zentraler Baustein des modernen Arbeitsplatzes.

Sicherheit im klassischen Büro: Vertrauen auf physische Grenzen

Früher waren Unternehmensnetzwerke wie Festungen aufgebaut: Wer sich innerhalb der Büroräume — also innerhalb des Sicherheitsperimeters — befand, galt automatisch als vertrauenswürdig. Dieses Konzept war effektiv, als die Systeme im Büro statisch waren und alle User dieselbe Infrastruktur nutzten.

Im herkömmlichen perimeterbasierten Netzwerksicherheitsmodell wird das Endgerät durch die Verbindung zum Büro des Unternehmens in das vertrauenswürdige Netzwerk eingebunden:



Wer sich also mit dem Netzwerk verbindet, hat Zugriff auf sämtliche Anwendungen, Ressourcen und Daten darin. Um zu verhindern, dass unautorisierte User oder Geräte ins vertrauenswürdige Netzwerk gelangen, kann ein Tool wie Network Access Control (NAC) eingesetzt werden, das den Netzwerkzugriff steuert— etwa indem nur Geräte mit einem von der PKI ausgestellten Zertifikat zugelassen werden.

Das ist zwar ein Schritt in die richtige Richtung, lässt jedoch hinsichtlich eines Sicherheitsmodells mit Segmentierung und minimalen Zugriffsrechten zu wünschen übrig. Denn dieser Ansatz beinhaltet:

- Umfangreichen, uneingeschränkten Zugriff
- Begrenzte, granulare Kontrollen
- Interne Netzwerkschwachstellen

Diese Merkmale eines Sicherheitsansatzes mit vertrauenswürdigem Netzwerk — weitreichende Zugriffsrechte, eingeschränkte Segmentierung und die inhärente Auffindbarkeit interner Netzwerke — passen nicht mehr zu der heutigen komplexen Bedrohungslandschaft. Angesichts immer raffinierterer Cyberangriffe, interner Bedrohungen und der zunehmenden Nutzung von Remotezugriffstools stoßen perimeterbasierte Sicherheitsmodelle an ihre Grenzen. Angreifer nutzen die Schwächen veralteter Architekturen aus, umgehen unzureichende Segmentierungskontrollen und bewegen sich lateral durch das Netzwerk. Dabei verwenden sie oft gültige Anmeldeinformationen, um unentdeckt zu bleiben. Die heutige Situation verlangt einen grundlegenden Wandel: Statt auf ein Netzwerk, das automatisch Vertauen gewährt, setzt Zero Trust auf die dynamische Überprüfung und Validierung jedes Zugriffsversuchs aller User, Geräte und Anwendungen.

Unternehmen benötigen einen Ansatz, der:

- den Zugriff gezielt auf einzelne Anwendungen begrenzt
- eine dynamische Durchsetzung von Richtlinien auf der Grundlage von Identität und Gerätezustand gewährleistet
- eine kontinuierliche Bewertung ermöglicht, bei der jeder Zugriff einzeln geprüft wird

Und das ist keine Zukunftsvision. Diese Architektur ist bereits verfügbar: die Zero-Trust-Netzwerkarchitektur, ein Konzept, dass speziell für Remote-Arbeit entwickelt wurde.

Ihr Zero-Trust-Arbeitsplatz

Mit der zunehmenden Remote-Arbeit verlagerten sich die Anwendungen in die Cloud, wodurch das herkömmliche vertrauenswürdige Netzwerk obsolet wurde. Der Zero-Trust-Ansatz, der das Prinzip des impliziten Vertrauens durch eine permanente Überprüfung ersetzt, erwies sich als effizientester Weg, um Usern den benötigten Zugriff bereitzustellen.

Mit der Rückkehr an den Arbeitsplatz wird Zero Trust noch wichtiger. In den letzten Jahren wurden die meisten Anwendungen und IT-Services in die Cloud migriert, was zu Produktivitätssteigerungen und effizienteren Betriebsabläufen geführt hat. Die Rückkehr zu veralteten, perimeterbasierten Strategien aus der Zeit vor der Cloud ist kontraproduktiv und mit dem modernen Arbeitsplatz nicht vereinbar.

Zero Trust ist mehr als eine Optimierung der Sicherheit — es ist eine strategische Chance, das moderne Büro neu zu erfinden und zukunftssicher zu machen. Mit Zero Trust profitieren Unternehmen von gesteigerter Agilität, höherer Skalierbarkeit und reduzierten Kosten. Ob bei der Einrichtung einer neuen Niederlassung, dem Aufbau temporärer Collaboration-Hubs oder der Verwaltung hybrider Teams — Zero Trust macht teure Netzwerkinstallationen wie MPLS oder von Telekommunikationsanbietern verwaltete Lösungen überflüssig. Gleichzeitig sinkt die Abhängigkeit von komplizierter On-Premise-Sicherheitsinfrastruktur.

Das Wichtigste: Zero Trust gewährleistet, dass Sicherheitsmaßnahmen stets zeitgemäß und wirksam sind. Da sich Tools und Workflows kontinuierlich weiterentwickeln, können Organisationen mit Zero Trust als Grundlage neue Technologien nahtlos integrieren, ohne durch veraltete Netzwerkkonfigurationen ausgebremst zu werden. Sie können sich dauerhaft von Firewalls und anderen veralteten Appliances verabschieden und ihre Sicherheitsstrategie zukunftssicher gestalten.

Die User sind wieder im Büro, Ihre Anwendungen jedoch nicht

Heutzutage erledigen die meisten Mitarbeiter ihre Aufgaben über Cloud-Anwendungen — selbst direkt in der Unternehmenszentrale. Das Büro fungiert heute nicht mehr als zentraler Knotenpunkt aller IT-Ressourcen. Tatsächlich erfolgt der Zugriff auf Ressourcen bei Mitarbeitern im Büro heute genauso wie bei Remote-Beschäftigten.

Dieser grundlegende Wandel hat mehrere Herausforderungen mit sich gebracht:

- **Büros als Konnektivitätsengpässe:** Mitarbeitende, die ins Büro zurückkehren, leiten Cloud-Traffic oft durchs Unternehmensnetzwerk, was zu unnötigen Latenzen und Störungen führt.

- **Verschlechterte User Experience:** Mitarbeiter können bei der Arbeit im Büro im Vergleich zu ihrer Remote-Arbeitsumgebung eine verminderte Anwendungsperformance feststellen. Das Problem liegt nicht immer am Netzwerk — es kann sich um verschiedene Ursachen handeln, von einer langsamen DNS-Auflösung bis hin zu einem unzureichend optimierten WLAN. Ohne Transparenz ist die Ermittlung der Ursache für die IT-Abteilung jedoch ein schwieriges Unterfangen.

- **Unzusammenhängende Monitoring-Tools:** Ältere Monitoring-Lösungen messen meist nur, ob das Netzwerk funktioniert, und vernachlässigen userzentrierte Kennzahlen wie Performance, Latenz oder Endgerätezustand.

Ein neuer Ansatz für Büronetzwerke

Stellen Sie sich ein Internetmodell wie im Café vor — Mitarbeitende verbinden sich einfach und direkt, genau wie im Homeoffice. Dieser Ansatz mag zunächst wie ein grundlegender Paradigmenwechsel erscheinen, lässt sich jedoch mit der Zero-Trust-Netzwerkarchitektur bereits realisieren.

In diesem Modell entsteht durch die Netzwerkverbindung kein automatisches Vertrauen. Das bedeutet: Auch die Arbeitsplätze im Büro gelten nicht automatisch als vertrauenswürdig. Sie werden genauso abgesichert wie die Geräte von Remote-Mitarbeitern — mit denselben Zugriffsrichtlinien.

Grundsätzlich gilt: Wer ins Büro kommt und sich ins Netzwerk einwählt, sollte keinen erweiterten Zugriff auf Anwendungen oder Ressourcen haben — genauso wie zu Hause über den eigenen Internetanschluss. Das Netzwerk sollte lediglich als Transportmedium dienen, ohne dass automatisch Berechtigungen gewährt werden.

Zugriff und Autorisierung richten sich nach der Identität des Users, dem verwendeten Gerät und der Anwendung, nicht nach der IP-Adresse. Jede Zugriffsentscheidung wird von einem Policy Enforcement Point — nicht von herkömmlichen Firewall-ACLs — getroffen. Dieser entscheidet nach dem Erforderlichkeitsprinzip, welche User auf welche Anwendungen und von welchen Geräten aus zugreifen dürfen.

Dieser Architekturwandel erfordert auch ein Umdenken.

1. **Erweitern Sie die Zugriffsrichtlinien auf On-Premise-User:** Die Zugriffsrichtlinie gilt für den User, nicht für das Netzwerk, mit dem er verbunden ist.

2. **Steigen Sie von Netzwerkzugriff auf Ressourcenzugriff um:** Mit Zero Trust gelangen User über richtlinienbasierte, identitätsorientierte Verbindungen direkt zu den Anwendungen. Dadurch entfällt die Notwendigkeit, umfassenden Zugriff auf das Netzwerk selbst zu gewähren.

3. **Behandeln Sie das Büronetzwerk wie das Internet:** Ihr Büro-WLAN funktioniert wie im Café. Es verbindet User einfach mit der Zero Trust Exchange, wo die Sicherheitsrichtlinien greifen. Kein eingehender Traffic. Kein implizites Vertrauen.

4. **Kontinuierliche Validierung des Vertrauens:** Zero Trust wertet jede Zugriffsanforderung dynamisch aus und überwacht Gerätestatus, Kontext und Risikosignale.

Das Besondere an Zero Trust: die konsistente Sicherheit. Mitarbeiter müssen sich keine Gedanken darüber machen, ob sie On-Premise oder remote arbeiten. Sie greifen auf die gleiche Weise auf Anwendungen zu, unabhängig davon, wo sie sich befinden. Diese einheitliche User Experience gewährleistet nicht nur optimale Produktivität, sondern vereinfacht auch die IT-Verwaltung.

Verbesserte Transparenz

Ein robustes Zero-Trust-Framework ermöglicht reibungslose Produktivität und beseitigt die Risiken, die durch implizites Vertrauen und veraltete Infrastrukturen entstehen. Um die Performance zu optimieren und Probleme rasch zu beheben, ist Transparenz eine ebenso zentrale Fähigkeit wie Identitätsmanagement, Monitoring des Gerätezustands und Anwendungskontrolle. Durch umfassende Transparenz sind IT-Teams in der Lage, die Bereitstellung von Anwendungen gezielt zu optimieren, Ausfälle zu reduzieren und Fehler durch präzisere Ursachenanalyse rascher zu beheben. Mit durchgängiger Transparenz — vom Endgerät bis zur Zielanwendung — können Administratoren Probleme in Sekunden einordnen: Liegt es am User, an der Verbindung oder an der Cloud?

Wenn Teams wieder gemeinsam im Büro arbeiten, sind diese Szenarien besonders wichtig:

- **Das WLAN-Dilemma im Büro:** Ein Mitarbeiter kommt zurück ins Büro und verbindet seinen Laptop mit dem Firmen-WLAN. Doch plötzlich läuft Microsoft Teams schleppend — dabei funktionierte es zu Hause über die einfache Breitbandverbindung perfekt. Woran liegt's? Schlechte WLAN-Abdeckung? Verzögerung im DNS? Oder ein Problem beim Teams-Server?

- **SaaS-Latenz durch Backhauling übers Unternehmensnetzwerk:** Eine Mitarbeiterin greift von ihrem Schreibtisch aus auf ein SaaS-basiertes CRM wie Salesforce zu. Da der Cloud-Traffic über das Unternehmensnetz geleitet wird, entsteht durch den Umweg (Backhaul) spürbare Latenz.

- **Transparenzlücken bei hybriden Belegschaften:** Ein weltweit tätiges Unternehmen hat Mühe, den Überblick über Gerätezustand, SaaS-Performance und ISP-Leistung zu behalten — egal, ob Mitarbeiter remote oder im Büro tätig sind. Die Folge: immer neue Support-Tickets, die die IT stark belasten.

Ein entscheidender Schritt zum Zero-Trust-Büro besteht darin, Digital Experience Monitoring fest in die Zero-Trust-Architektur zu integrieren.

Warum gerade Zscaler das Zero-Trust-Büro möglich macht

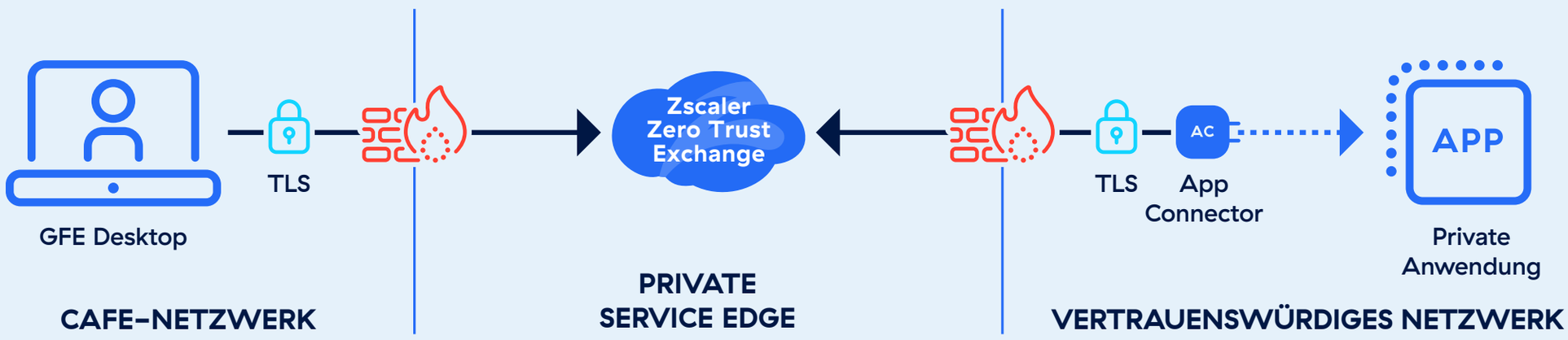
Zscaler hat sich als verlässlicher Partner für Behörden bewährt, die Modernisierungsvorhaben umsetzen. Als branchenführender Anbieter von Cloud-Sicherheitsservices genießt Zscaler das Vertrauen von 14 von 15 Ministerien, darunter das DHS, das DOJ und die GSA, wenn es darum geht, Netzwerke zu absichern, Abläufe zu vereinfachen und Kosteneinsparungen zu erzielen. Wir gewährleisten die Sicherheit von Millionen von Usern in mehreren hundert staatlichen Institutionen, von lokalen bis hin zu nationalen Behörden.

Zscaler für User bietet drei zentrale Funktionen, die Risiken minimieren, die Produktivität erhöhen und Kosten sowie Komplexität reduzieren.

- **Sicherer Internet- und SaaS-Zugriff (ZIA):** Hierüber greifen Ihre Mitarbeiter auf Internet und Anwendungen zu und sind dabei zuverlässig vor Cyberbedrohungen und Datenverlust geschützt.

- **Sicherer Zugriff auf private Anwendungen (ZPA):** Stellt sicher, dass User über die lokale Private Service Edge verbunden sind und die Datenverbindung zu einer privaten Anwendung direkt über das Behördennetzwerk vermittelt wird — ohne Umweg über das Internet.

- **Digitale User Experience (ZDX):** Liefert volle Transparenz über die digitalen Erfahrungen der Mitarbeiter — vom Endgerät bis zur SaaS-Anwendung — und sorgt so für reibungslose Betriebsabläufe, egal ob im Büro oder remote.



Moderne Arbeitsumgebungen dank Zero Trust

Mit dem Wandel der Arbeitswelt verliert die Vorstellung vom traditionellen Büro zunehmend ihre Bedeutung. Unabhängig davon, ob Mitarbeiter in Büros, im Homeoffice oder mobil arbeiten, muss ihre Erfahrung konsistent und sicher sein.

Mit der Rückkehr der Mitarbeiter ins Büro erhalten Organisationen eine einmalige Chance, ihre Arbeitsplatzinfrastruktur zu modernisieren. Eine Zero-Trust-Grundlage sorgt nicht nur für mehr Sicherheit, sondern auch für Skalierbarkeit, Flexibilität und dauerhafte Resilienz. So sieht ein optimales Zero-Trust-Büro aus — ein Arbeitsplatz, an dem die Produktivität aufblüht.

Und das ist schon heute problemlos realisierbar. Indem Organisationen dieselben Prinzipien, die für Remote-Arbeit gelten, auch auf den Büroalltag anwenden, können sie Risiken deutlich reduzieren, die User Experience verbessern und eine zukunftssichere Sicherheitsarchitektur schaffen.

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die Zscaler Zero Trust Exchange™ schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlusten. Als weltweit größte Inline-Cloud-Sicherheitsplattform wird die SASE-basierte Zero Trust Exchange™ in über 150 Rechenzentren auf der ganzen Welt bereitgestellt. Weitere Informationen erhalten Sie auf **www.zscaler.com/de**. Gerne können Sie uns auch auf X folgen **@zscaler**.

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

zscaler™

Zero Trust Everywhere