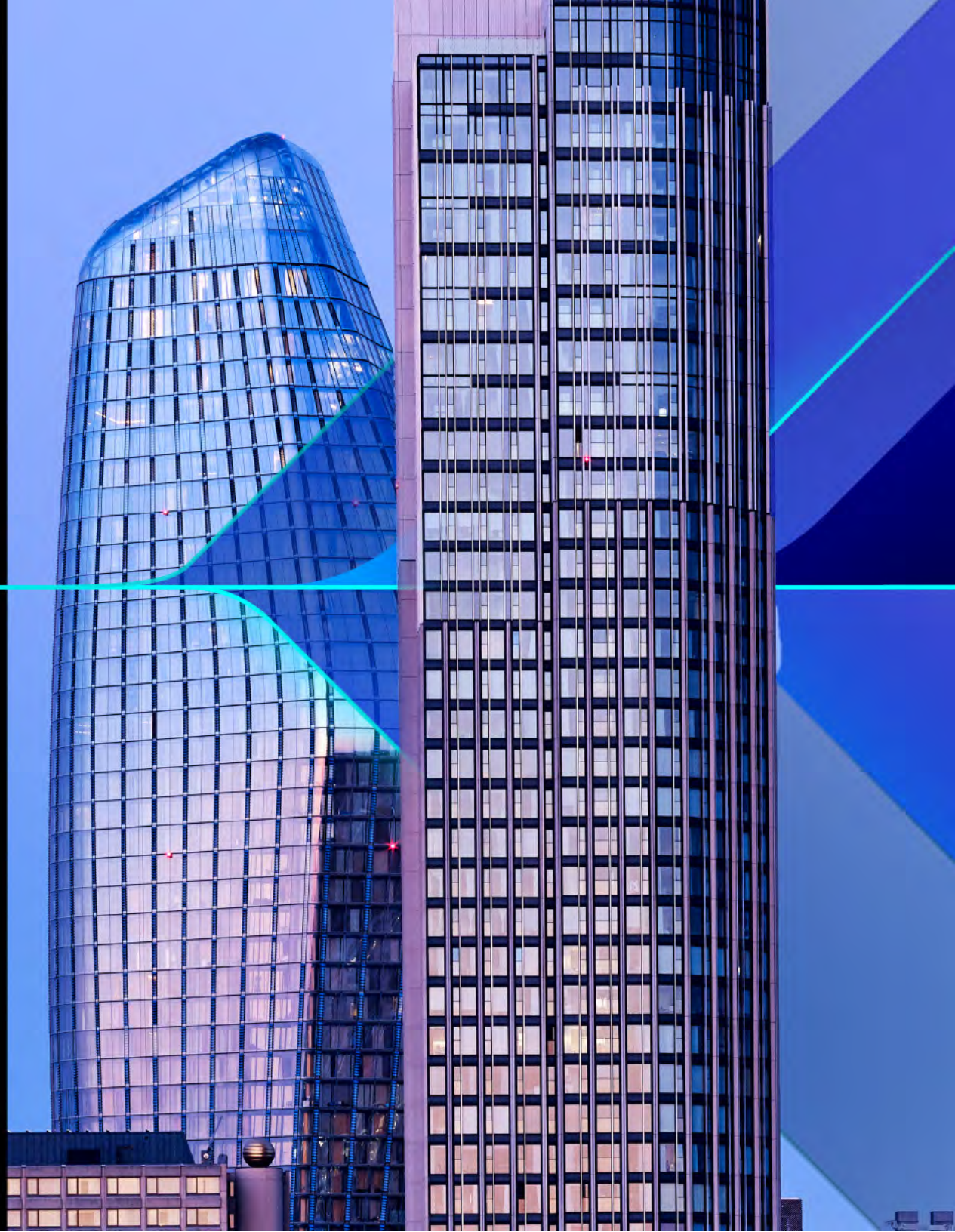
ZSCALER

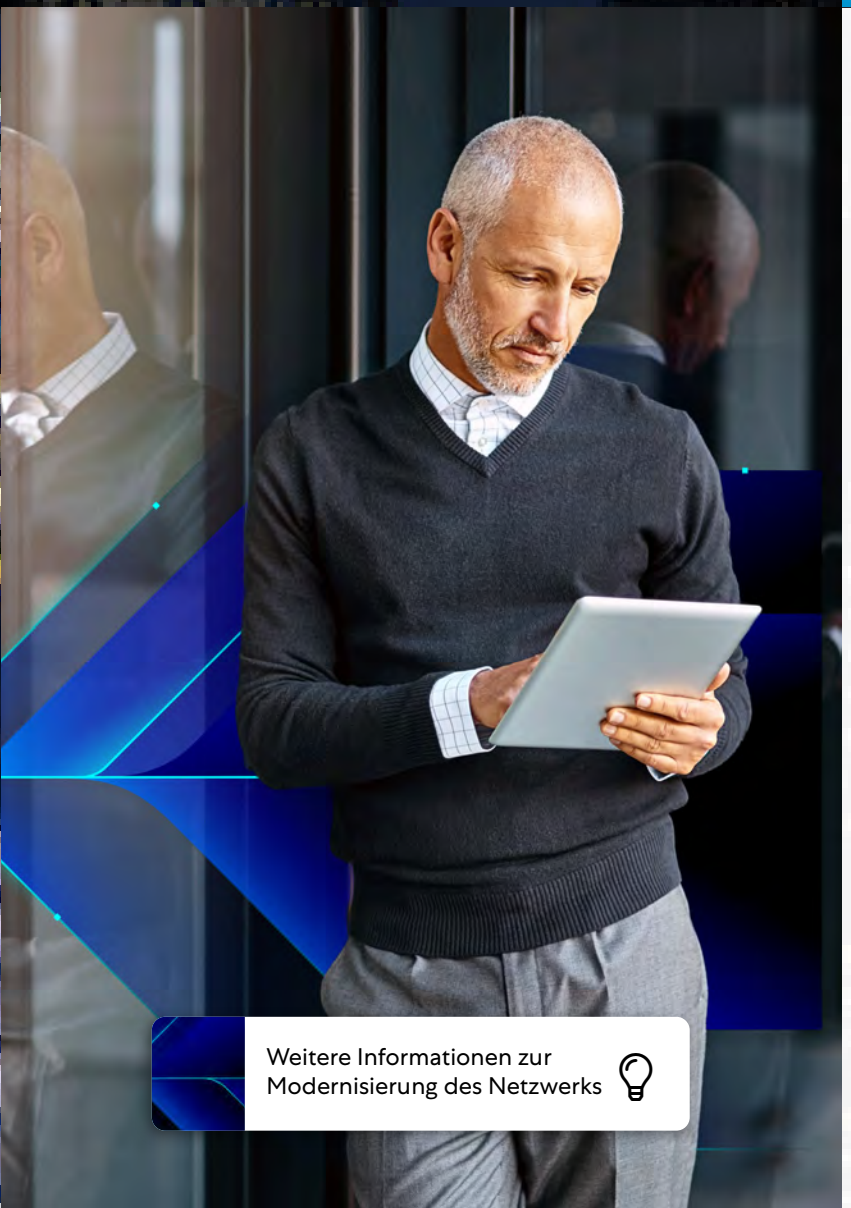
FÜR BANKWESEN UND FINANZ-DIENSTE



INHALT

1 DIE TECHNOLOGIE-LANDSCHAFT **VERÄNDERT SICH**

Immer wenn irgendwo auf der Welt disruptive Ereignisse stattfinden, reagiert vor allem ein Branchensegment ebenso rasch wie sensibel darauf: der Finanzdienstleistungssektor.



Weitere Informationen zur Modernisierung des Netzwerks

Die Wirtschaft in diesem Markt ist geprägt von kontinuierlichen Veränderungen und wird stark beeinflusst von internationalen Faktoren. Schon deshalb verfolgen Finanzdienstleister in der Regel einen ganzheitlichen und strategischen Ansatz. Sie nutzen die Vorteile neuer Fintech-Plattformen in der Cloud und profitieren von dem Boom mit mobilen Endgeräten und neuesten Innovationen in der KI-gestützten Automatisierung. Kurz: Der Finanzdienstleistungssektor musste sich neu erfinden.

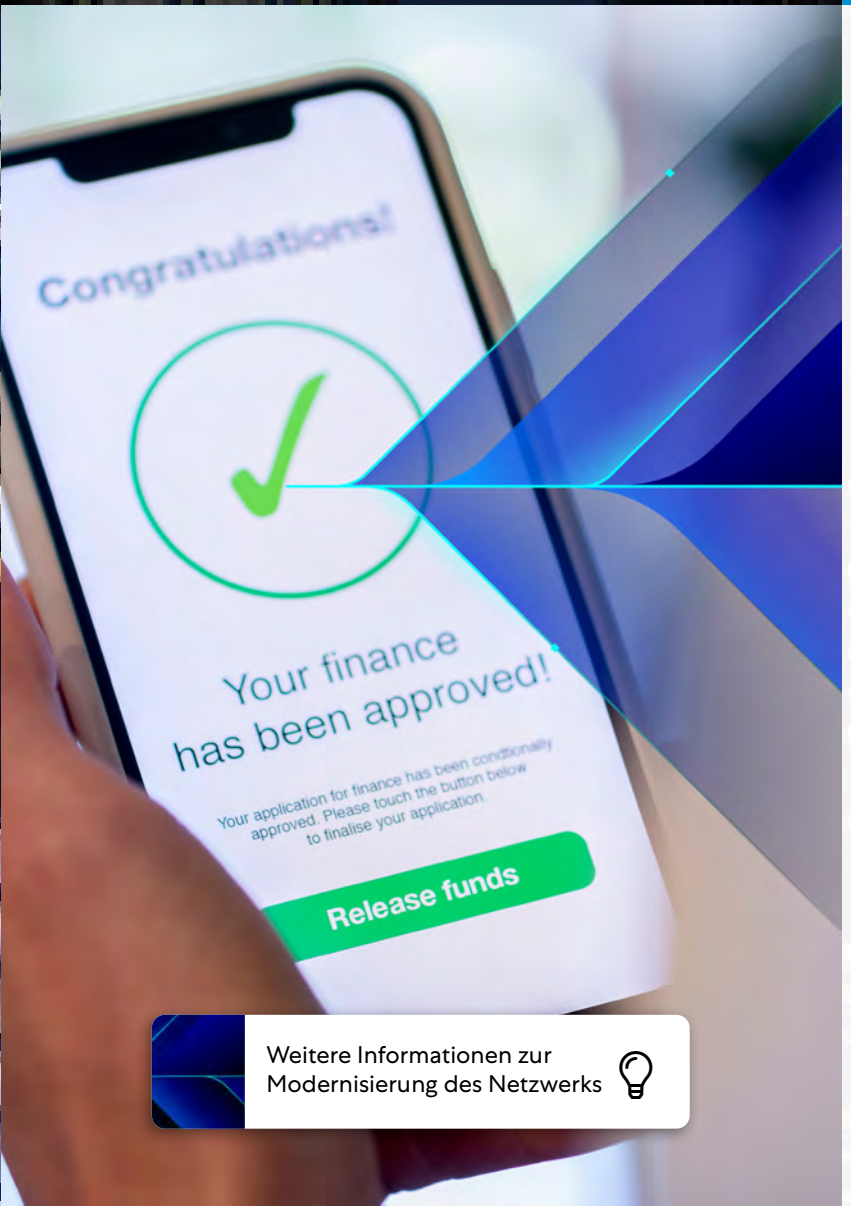
Waren es bis vor Kurzem noch vor allem die so genannten Millennials, die für den Siegeszug der neuen Bankentechnologien wie kontaktlose „Tap & Pay"-Systeme sorgten, so haben solche Innovationen in den letzten Jahren ein immer breiteres Publikum erreicht. Heute nutzen alle Altersgruppen Möglichkeiten wie das kontaktlose Bezahlen. Aber auch die COVID-19-Pandemie hat der Umstellung auf Online-Banking Vorschub geleistet und die bargeldlose Gesellschaft salonfähig gemacht.

Gleichzeitig sorgen technologische Innovationen für neue Chancen im Markt. Das Aufkommen sogenannter Challenger-Banks beispielsweise ist eng mit der Bereitschaft von Verbrauchern verknüpft, E-Commerce-Technologien mit Smartphones und über elektronische Zahlungssysteme zu nutzen.

Ob es um eine Hypothek, eine Versicherung, einen Investitionsplan, um Überweisungen oder um alltägliche Girokonto-Aktivitäten geht – digital ist in. Die Dynamik des Marktes und die gewaltige Auswahl an Möglichkeiten hat zudem dazu geführt, dass Kunden äußerst anspruchsvoll geworden sind. Sie erwarten ein nahtloses Benutzererlebnis in Echtzeit und einen individuellen Mehrwert.

2 AKTUELLER STAND DER DIGITALEN TRANSFORMATION

Digitale Innovationen und geschäftliche Agilität sind und bleiben also die Voraussetzungen dafür, neue Kunden gewinnen, den Marktanteil ausbauen und Wachstumschancen nutzen zu können.



Das Problem dabei: Viele etablierte Finanzunternehmen nutzen proprietäre Kernsysteme in lokalen Rechenzentren. Diese Systeme wurden im Laufe der Jahre individuell angepasst. So sind zahlreiche Abhängigkeiten zwischen unterschiedlichsten IT-Funktionen auf mehreren Ebenen entstanden. Hinzu kommt, dass unzählige Finanzvorschriften, Governance-Kontrollen und Datenschutzgesetze den Umstieg in moderne Systemtopologien wie die Cloud erschweren.

Auf der anderen Seite entstehen mehr und mehr Standards und Richtlinien für das Cloud-Computing. Sie sorgen dafür, dass die für Banken essentiellen Themen Sicherheit und Datenschutz höchste Aufmerksamkeit erhalten. So sind Finanzinstitute in der Lage, neue Innovationen zu nutzen, und gleichzeitig der Compliance Rechnung zu tragen. Mittlerweile arbeiten viele Finanzinstitute in einer hybriden Umgebung: Neben den gewohnten Legacy-Infrastrukturen kommt immer öfter auch Cloud-IT zum Einsatz – mit Plattformen und Lösungen für verschiedenste Anwendungsbereiche, für das ERP, Marktdaten, CRM-Forschung, Vertriebsmaßnahmen und sogar Marktanalysen. Selbst einfache Schulungen für FINRA-Qualifikationen finden online statt, spätestens, seitdem die **FINRA 100 Prozent ihrer eigenen Anwendungen in die Cloud verlagert hat.**

Es verwundert also nicht, dass die digitale Transformation auch im Finanzdienstleistungssektor angekommen ist. Laut einer von Zscaler im Jahr 2020 durchgeführten Umfrage unter 600 EMEA-CIOs verfolgen viele Unternehmen aus diesem Branchensegment inzwischen sogar eine Cloud-first-Strategie. Sie nutzen mehrere öffentliche Clouds und SaaS-Applikationen (Software-as-a-Service) für kundenseitige Lösungen, Backoffice-Abläufe und Integrationen mit Partnern im Finanzökosystem wie Shadow Banks oder Fintech-Anbieter.

Demnach haben zwei Drittel der Unternehmen 50 Prozent ihrer Anwendungen bereits in die Cloud verschoben, bei einem Viertel der Interviewten arbeiten sogar schon 75 Prozent der Lösungen in der Wolke.

Weitere Informationen zur Modernisierung des Netzwerks

3 DIE DIGITALE TRANSFORMATION MEISTERN

Finanzdienstleistungen verlagern sich also immer mehr von der lokalen Hausbank ins Internet. Etablierte Anbieter stehen in diesem Zusammenhang allerdings vor der Herausforderung, künftig dasselbe Niveau für den Kundenservice zu gewährleisten – schon deshalb, um das Risiko einer Kundenabwanderung zu minimieren.

Das Kalkül dahinter: Werden Services korrekt und nahtlos bereitgestellt, stellen Kunden auch mehr Fragen. Sie interagieren mehr und kaufen neue Dienstleistungen. Werden diese Services hingegen fehlerhaft, langsam oder auf nicht vertrauenswürdige Weise bereitgestellt, sind Klienten im Handumdrehen bei der Konkurrenz.

Ebenso wie in anderen Branchen spielen auch im Finanzdienstleistungssektor neue Technologien eine entscheidende Rolle für den Fortschritt. Hierzu gehören derzeit vor allem Technologien, die sich auf Innovationen wie 5G, KI, Blockchain oder Robotic Process Automation (RPA) stützen und die immer umfangreichere Anwendungsmöglichkeiten des Internet of Things (IoT) nutzen.

Und dann kam Corona: Viele dieser ersten Maßnahmen zur Einführung, Implementierung und Nutzung moderner Technologien mussten durch die Auswirkungen von COVID-19 abrupt gestoppt werden. Die Pandemie brachte wirtschaftliche und organisatorische Entwicklungsstrategien auch in diesem Branchensegment ins Wanken. Unternehmen weltweit mussten sich in aller Eile auf die neuen Gegebenheiten einstellen und sich auf die Geschäftskontinuität konzentrieren. Größtenteils mit Erfolg: Innerhalb weniger Wochen hatten die meisten IT-Abteilungen die neue Herausforderung bewältigt und ihr Projektmanagement optimiert. Möglich wurde das, indem Projekte neu priorisiert und beschleunigt wurden, damit die lokale und internationale Wirtschaft weiterlaufen konnte. Tausenden Büro- und Filialmitarbeitern wurde in diesem Zusammenhang die Möglichkeit geboten, im Homeoffice zu arbeiten, während gleichzeitig bargeldlose Zahlungen und andere Formen für **reibungslose Remote-Prozesse** rasch eingeführt wurden – einige sogar vor dem ursprünglich geplanten Starttermin.

Weitere Informationen zur Modernisierung des Netzwerks

4 LEGACY-INFRASTRUKTUR: WEGBEREITER ODER HÜRDE?

Doch obwohl viele Finanzdienstleistungsunternehmen im Fahrwasser der digitalen Transformation erste große Fortschritte erzielen und so die Vorteile der Cloud und mobiler Lösungen nutzen, entstehen immer wieder neue Herausforderungen.

Ein typischer Grund im Finanzumfeld ist nicht selten das Never-change-a-runnings-system-Prinzip: Bestehende Systeme werden häufig bis ans äußerste Ende ihrer Lebensdauer genutzt. Das Problem dabei ist, dass Legacy-Infrastrukturen nicht für die transaktionalen, analytischen und prozessualen Anforderungen der modernen Cloud- und Mobility-orientierten Welt entwickelt wurden – Defizite, die während der Pandemie deutlich zum Vorschein kamen.

So waren vor der Krise die meisten Mitarbeiter im Finanzdienstleistungssektor in einer Filiale oder einem Büro tätig. Nur Wenige unternahmen Geschäftsreisen, um Besprechungen vor Ort abzuhalten, oder arbeiteten von zu Hause aus. Hier kamen vornehmlich Technologien wie Virtual Private Networks (VPN) oder Virtualized Desktop Interfaces (VDI) für die wichtigsten Banksysteme zum Einsatz. Während der Pandemie mussten IT-Abteilungen umdenken und praktisch über Nacht einen sicheren Remote-Access für eine Rekordzahl von Mitarbeitern realisieren. Sie waren plötzlich gezwungen, im Homeoffice zu arbeiten.

Mobile Mitarbeiter konnten so weiterhin auf Geschäftssysteme und Cloud-Anwendungen zugreifen. Allerdings waren die VPNs nicht darauf ausgelegt, von so vielen Mitarbeitern genutzt zu werden. Das war schon deshalb nicht möglich, weil der Traffic einen Stack von Appliances wie Load Balancer, DDoS, Firewalls und VPN-Konzentratoren durchlaufen musste. Anders ausgedrückt: Das so genannte Backhauling von Traffic über das bestehende Netzwerk, die Legacy-Infrastruktur und mehrere Appliances führte zu Latenzen, Frustration bei Usern und geringerer Produktivität. Im schlimmsten Fall umgingen Mitarbeiter Sicherheitsrichtlinien und VPN-Kontrollen, was wiederum zu gefährlichen Sicherheitslücken führte.

Mittels VDI-Technologie waren Remote-Benutzer über ihre privaten Geräte (Bring-Your-Own-Device – BYOD) unter Umständen auch in der Lage, Verbindungen zu den wichtigsten Systemen, E-Mails und anderen Anwendungen herzustellen und so klassische Probleme wie die Exposition oder den Diebstahl von Daten zu verringern. Diese Lösungen sind jedoch nicht nur äußerst schwierig einzurichten und kostspielig in der Wartung, sie wurden während der Pandemie auch überstrapaziert und zu einem zusätzlichen Sicherheitsrisiko.

Weitere Informationen zur Modernisierung des Netzwerks

IT-Unternehmen kompensieren ein leistungsschwaches Netzwerk typischerweise mit zusätzlicher Infrastruktur. Doch dadurch steigen nicht nur die Komplexität und die Kosten, sondern auch die Sicherheitsrisiken. Je weiter Unternehmen diesen Weg voranschreiten, desto mehr leidet ihre Agilität, Innovationskraft und Wettbewerbsfähigkeit.

Dieser Trend hat sich mit COVID-19 in den letzten Monaten beschleunigt: Ein Großteil der Mitarbeiter arbeitet im Homeoffice, dafür musste die Finanzdienstleistungsbranche von jetzt auf gleich Sofwarelösungen wie Microsoft 365 bereitstellen.

DARAUS ERGEBEN SICH EINIGE HERAUSFORDERUNGEN:

- Auf VPNs basierende Remote-Access-Lösungen sind nicht in der Lage, die geforderten Service Levels zu gewährleisten, was zu Latenzen und einer schlechten Anwendererfahrung führt.
- VPN-basierter Remote-Access, der Heim-PCs ins Unternehmensnetzwerk einbindet, stellt nachweislich den Hauptvektor für Infektionen von Endgeräten dar. Dies verschärft sich durch die vermehrte Arbeit im Homeoffice.
- Microsoft 365 benötigt zur Gewährleistung akzeptabler Service Levels eine höhere Bandbreite und eine niedrigere Latenz.
- Die Erweiterung der „Hub and Spoke"-Architektur ist sehr kostspielig und bietet letztlich nicht das erforderliche SLA.
- Die großflächige Ausweitung von bestehenden Sicherheitsarchitekturen macht Unternehmen insbesondere für Trojaner-Angriffe anfälliger und schützt gleichzeitig nicht gänzlich vor Insider-Bedrohungen.

Vielen IT-Führungskräften ist bewusst, dass „Hub and Spoke"-Architekturen mit den verteilten Cloud- und Mobile-Umgebungen nicht mithalten können. Sie unterstützen Remote-Benutzer nicht ausreichend und bieten nicht die nötige Skalierbarkeit für den wachsenden Netzwerk-Traffic. Ebenso beansprucht die Sicherung von Legacy-Infrastrukturen extrem viel Zeit, Energie und finanzielle Ressourcen. In diesem Zusammenhang rückt die Notwendigkeit einer Transformation der Architektur immer stärker in den Vordergrund. Hinzu kommt: Die IT muss eine Architektur entwerfen und implementieren, die eine Fülle von neuen Innovationen in vielfältigen, dynamischen und komplexen Umgebungen unterstützt.

Ziel muss es sein, eine digitale Welt ins Leben zu rufen, die natürliche Sprache versteht und verarbeitet, große Datenmengen sammelt, Muster erkennt, interpretiert, wahrnimmt, schlussfolgert und in Echtzeit berät – denn so eine digitale Welt unterstützt gesteuertes Lernen, Betriebstechnologie, Robotik und Wearables der nächsten Generation.

5 SPAGAT ZWISCHEN SICHERHEIT UND OPTIMALER ANWENDERERFAHRUNG

Banken, Versicherungen und andere Finanzdienstleister sind für die Aufbewahrung und Verwaltung riesiger Mengen an Kundenkonten und Finanzinformationen zuständig.

Angesichts der Herausforderung, Kriminellen und ihren ständig neuen Meth- oden immer einen Schritt voraus zu sein und die strengen Finanzvorschriften einzuhalten, überrascht es kaum, dass Finanzunternehmen zu denjenigen Unternehmen gehören, die am meisten für Cyber-Sicherheit ausgeben.

Denn neue Entwicklungen im Digitalbereich eröffnen auch Kriminellen neue Möglichkeiten, Schwachstellen auszunutzen. Mitarbeiter, die auf eine Phishing-E-Mail antworten, können ihre Zugangsdaten gefährden und Opfer einer Datenschutzverletzung oder eines Ransomware-Angriffs werden. Es stellt sich also die Frage nach der richtigen Balance: Wie können Finanzunternehmen ihrer mobilen Remote-Belegschaft die wichtigsten Geschäftsprozesse und -anwendungen kostengünstig und sicher bereitstellen, ohne die Anwendererfahrung zu beeinträchtigen?

Bei zu vielen einzelnen Sicherheitsvorkehrungen leidet die Anwendererfahrung erheblich. Kunden und Mitarbeiter sind frustriert, die Produktivität sinkt. IT-Führungskräfte wissen, dass sie sowohl für die Sicherheit als auch für die Anwendererfahrung zuständig sind, kämpfen aber damit, beiden Aspekten gleichermaßen gerecht zu werden.

Weitere Informationen zur Zscaler Zero Trust Exchange

6 BALANCE ZWISCHEN SICHERHEIT UND ANWENDERERFAHRUNG: SASE UND ZERO TRUST

Secure Access Service Edge (SASE) ist ein von Gartner definiertes Modell, das speziell für die Bewältigung von Sicherheitsherausforderungen entwickelt wurde, die sich durch Apps, Geräte und User stellen, die sich außerhalb des traditionellen Netzwerkperimeters befinden.

Weitere Informationen zur Zscaler Zero Trust Exchange

Die SASE-Architektur kombiniert umfassende WAN- und Netzwerksicherheitsfunktionen wie Secure Web Gateway, CASB, Firewall as a Service und Zero Trust Network Architecture (ZTNA) und ermöglicht es digitalen Unternehmen, ihren Bedarf an dynamischem und sicherem Zugang zu decken.

Im Gegensatz zu einem herkömmlichen Netzwerkzugriff vermitteln adaptive Zero-Trust-Lösungen Verbindungen und gewähren damit einen granularen Zugriff auf Basis von User, Gerät, Standort und App. So profitieren autorisierte Anwender von einem schnellen und sicheren Zugriff, unabhängig davon, wo sie sich befinden. Ein weiterer Vorteil: Anwender müssen nicht „ins Netzwerk" platziert werden. Vielmehr wird das Internet mit ZTNA als nicht vertrauenswürdiger Transportweg definiert, während der Zugriff auf Anwendungen über einen zwischengeschalteten Cloud-Service erfolgt, der von einem Drittanbieter oder einem selbst gehosteten Service kontrolliert wird.

Dieses Modell macht umständliche, herkömmliche VPN-Hardware und -Prozesse überflüssig und schafft einen nahtlosen Prozess für Anwender und somit ein besseres Gesamterlebnis.

Konkret bietet ZTNA einen kontrollierten Zugang zu Ressourcen und verbessert gleichzeitig die Konnektivität, weil Anwendungen nicht mehr direkt im Internet freigegeben werden müssen. Das reduziert die Angriffsfläche. Die Vorteile von ZTNA zeigen sich nicht zuletzt auch während der Pandemie: ZTNA wird aktuell in zahlreichen Unternehmen eingeführt, um es der Remote-Belegschaft und Mitarbeitern im Homeoffice zu ermöglichen, mit demselben Sicherheitsniveau auf wichtige Geschäftsanwendungen zuzugreifen, wie Mitarbeiter in der Zentrale. Daher gilt ZTNA heute als ein Best-Practice-Standard, der vielerorts unternehmensweit eingesetzt wird. Ganz egal, ob die User auf das Rechenzentrum, private Apps oder die öffentliche Cloud zugreifen, und unabhängig davon, ob sie im Büro oder remote arbeiten – die Anwendererfahrung ist immer identisch.

ZERO TRUST EXCHANGE

Zscaler Zero Trust Exchange ist eine speziell für die Cloud entwickelte SASE-Plattform, die Anwender, Geräte und Apps mittels Unternehmensrichtlinien über jedes beliebige Netzwerk sicher verbindet. Sie ist schnell, sicher und skalierbar und vereint höchste Sicherheit mit einer optimalen Anwendererfahrung. So wird die Cloud zu einem sicheren Ort für geschäftliche Aktivitäten.

7 ZSCALER – EINE EINFÜHRUNG

Sei es die Entwicklung neuer Banking-Lösungen, die mit Krypto-währungen und neuen grenzüberschreitenden Services arbeiten, die Bekämpfung von Betrug oder der Umgang mit neuen Prozessen zur Erfüllung gesetzlicher Auflagen – Finanzdienstleister müssen ihre Strategie auf einer modernen, robusten, agilen und skalierbaren Plattform aufbauen, um Innovationen rasch voranzutreiben und der Konkurrenz einen Schritt voraus zu bleiben.

Weitere Informationen zur Zscaler Zero Trust Exchange

Die SASE-basierte Zero-Trust-Exchange-Plattform von Zscaler ist seit über zehn Jahren in Betrieb und in mehr als 150 Rechenzentren weltweit verfügbar. Sie hat sich zur weltgrößten Inline-Cloud-Sicherheitsplattform entwickelt und stoppt täglich über 100 Millionen Bedrohungen (Stand: September 2020). Die Plattform verarbeitet mehr als 150 Milliarden Transaktionen und 175 Millionen Sicherheits-Updates pro Tag. Das entspricht dem Zehnfachen der Anzahl von Google-Suchanfragen pro Tag weltweit.

Zscaler hat sich vor allem auch im Finanzdienstleistungssektor bewährt: Über 500 Finanzdienstleister, sechs der zehn größten US-Banken, sieben der zehn größten europäischen Banken und zwei der fünf größten australischen Banken vertrauen auf Zscaler und betreiben ihre IT-Infrastruktur mit der Zscaler Zero Trust Exchange-Plattform. Insgesamt ist Zscaler zuverlässiger Partner für 4.500 Kunden in 185 Ländern, darunter 450 Top-Unternehmen der Forbes Global 2000. Unter Anwendung von Unternehmensrichtlinien schützt die Zero Trust Exchange tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust.

Die Plattform überlagert bestehende Architekturen und beschleunigt dadurch die digitale Transformation umgehend, indem effiziente, sichere, kundenorientierte und skalierbare Services bereitgestellt werden:

- **Effizient:** Vereinfacht die IT, reduziert Komplexität und Kosten.
- **Sicher:** Verbessert die Ausfallsicherheit und Security Posture, mindert Datenverluste und Sicherheitsrisiken, weil sich die Sicherheitslage mehrerer Abteilungen übersichtlich und kompakt in einer einzigen Benutzeroberfläche darstellen lässt.
- **Kundenorientiert:** Ermöglicht das Arbeiten von jedem beliebigen Standort aus, erhöht die Kapazität, reduziert Latenzen und schafft eine einheitliche Anwendererfahrung zur Verbesserung der Produktivität.
- **Skalierbar:** Eine moderne, agile Plattform – unterstützt digitale Innovationen, beschleunigt die digitale Transformation und schafft Kapazitäten für Wachstum.

Die National Australia Bank (NAB) bietet umfassende und integrierte Bank- und Finanzprodukte sowie -dienstleistungen, einschließlich Vermögensverwaltung. Sie verfügt über Niederlassungen in Australien, Neuseeland, Teilen Asiens, Großbritannien und den USA.

Angesichts des COVID-bedingten Lockdowns musste die Bank ihren Mitarbeitern schnell die Möglichkeit bieten, von zu Hause aus zu arbeiten, während gleichzeitig ihre Dienstleistungen für mehr als neun Millionen Kunden aufrechterhalten blieben.

„Vor der COVID-19-Pandemie waren es immer maximal 5.000 Mitarbeiter, die außerhalb unserer Büros arbeiteten", so Steve Day, EGM Infrastructure, Cloud and Workplace bei der NAB. „Innerhalb kürzester Zeit mussten wir einen Weg finden, um die Mitarbeiter unseres Contact Centers so auszustatten, dass sie von zu Hause aus Anrufe bearbeiten und auf unsere Apps und Datenspeicher zugreifen konnten", erklärt er. „Und als ob das alleine nicht schon genug wäre, hatten wir viermal so viele Anrufe zu bewältigen wie normalerweise."

In Zusammenarbeit mit Zscaler schaffte es die NAB in nur drei Wochen, einen sicheren Remote Access für mehr als 32.000 Mitarbeiter, einschließlich der Callcenter-Teams, bereitzustellen. Die NAB entschied sich für Zero Trust, um die Kosten und die Angriffsfläche zu reduzieren und gleichzeitig eine Infrastruktur zu entwickeln, die den zukünftigen Betrieb unterstützt.

„Zero Trust hat zwei große Vorteile: Erstens müssen wir kein separates Unternehmensnetzwerk mehr betreiben, was erhebliche Kosteneinsparungen nach sich zieht. Im neuen Modell bieten wir nur noch innerhalb unserer Niederlassungen einen öffentlichen Internetzugang. Zweitens haben wir unsere Security Posture erhöht, und zwar nicht durch die Anschaffung einer teureren Sicherheitsinfrastruktur, sondern indem wir alle Daten und Anwendungen aus der Unternehmensumgebung entfernt haben, um unsere Angriffsfläche zu verringern. Wir verfügen jetzt über eine sichere Netzwerkinfrastruktur, die die NAB sowohl während der aktuellen Krise als auch nach der Rückkehr zum Normalbetrieb unterstützen kann."

„Die Mitarbeiter schalten ihren PC im Homeoffice ein, und er funktioniert ganz genauso wie im Büro. Sie müssen sich keine Gedanken über zusätzliche Anmeldeschritte machen oder sich mit Sicherheits-Tokens herumschlagen. Es läuft einfach alles wie gewohnt", berichtet Steve Day, EGM Infrastructure, Cloud & Workplace.

National Australia Bank

National Australia Bank,
Melbourne, Australien

www.nab.com.au

8 FUSIONEN UND ÜBERNAHMEN

Fusionen, Übernahmen und Veräußerungen sind im Finanzdienstleistungssektor schon fast an der Tagesordnung, stellen für Netzwerk- und Sicherheitsteams jedoch eine ganz besondere Herausforderung dar. Das liegt in erster Linie daran, dass sie die Konnektivität von Usern zu internen Anwendungen und die Sicherheit sensibler Daten gewährleisten müssen.

Die Konvergenz unterschiedlicher Netzwerke, die Verwaltung überlappender IP-Adressen und die Umsetzung einheitlicher Sicherheitsstandards sind nur einige der Herausforderungen, mit denen die IT konfrontiert ist. Projekte sind zeitaufwändig und ressourcenintensiv und nehmen oft Monate oder gar Jahre in Anspruch.

Geschwindigkeit, Sicherheit und Anwendererfahrung stehen bei diesen komplexen Übergängen an erster Stelle. Durch die Zusammenarbeit mit Zscaler können Unternehmen M&A sowie Veräußerungen erheblich vereinfachen:

- Einfache Implementierung von Software, sodass User innerhalb von Minuten an Anwendungen weitergeleitet werden, ohne Netzwerke konvergieren zu müssen.
- Standardisierte Sicherheit für alle Assets. Anwendungen sind nur für autorisierte User sichtbar, und User befinden sich niemals im Netz.
- User haben unabhängig von Gerät, Anwendung oder Standort permanenten Zugang.

Weitere Informationen zur Zscaler Zero Trust Exchange

9 DER NÄCHSTE SCHRITT IN DER DIGITALEN TRANSFORMATION

Finanzunternehmen haben vergleichsweise schnell auf die Pandemie reagiert. Jetzt liegt es an den IT- und Sicherheitsteams, sicherzustellen, dass sie sich erfolgreich an die neue Normalität anpassen.

Weitere Ressourcen zum Thema „Work-from-Anywhere“

Es ist an der Zeit, die nächste Stufe der digitalen Transformation anzugehen. Damit ist der Aufbau einer modernen Infrastruktur, die zukünftige Innovationen ermöglicht, von größter Bedeutung.

Mit dem neuen Hochgeschwindigkeitsnetz 5G und dem vermehrten Einsatz von Operating Technologies, fortschrittlicher Robotik, Wearables und anderen kundenorientierten Innovationen kommen neue Herausforderungen auf den Finanzdienstleistungssektor zu. Das gleiche gilt für Sicherheitslücken. Die Cyber-Sicherheit wird somit eines der größten Risiken für Finanzinstitute bleiben.

Es wird in Zukunft immer wichtiger, mit vertrauenswürdigen Infrastrukturanbietern zusammenzuarbeiten, die sowohl den Anforderungen von heute gewachsen sind als auch die Vision und Fähigkeit haben, Finanzunternehmen weltweit den Weg in eine digitale Zukunft zu ebnen.

WARUM JETZT

10 HANDLUNGSBEDARF BESTEHT

Wenn Sie nichts tun, kommt Sie das teuer zu stehen – sei es in Form von höheren Infrastruktur- und MPLS-Kosten, Produktivitätsverlusten oder finanziellen Aufwendungen für die Behebung der Folgen eines Cyberangriffs.

Handeln Sie jetzt, sorgen Sie sofort für mehr Sicherheit, indem Sie die unternehmensweite Sicherheitslage übersichtlich und kompakt in einer einzigen Ansicht darstellen, während Sie gleichzeitig die neue Normalität der Remote-Arbeit effektiv unterstützen.

Gleichzeitig werden Ihre IT-Investitionen immer zukunftsorientierter und basieren auf skalierbaren, neuen Architekturen, die Geschäftsprioritäten und Innovationen beschleunigen können.

ERFÜLLUNG GESETZLICHER AUFLAGEN

Unabhängige Bankaufsichtsbehörden arbeiten daran, eine effektive und konsequente Regulierung und Aufsicht der Banken- und Finanzdienstleistungsbranche sicherzustellen. Diese Behörden haben unter Mitwirkung von branchenführenden Unternehmen Leitlinien und Empfehlungen für die Einführung von Cloud-Technologien entwickelt. Hinzu kommen Richtlinien für den Prozess und die Praxis der Auslagerung an Cloud-Service-Anbieter (CSPs) und die Einführung eines prinzipienbasierten Ansatzes für die Verwaltung und Messung von Risiken in Cloud-Technologieumgebungen.

Zscaler verpflichtet sich, Kunden auf ihrem Weg zu umfassender Compliance zu begleiten. Die robusten Sicherheits- und Datenschutzlösungen sowie die Unterstützung bei der Erfüllung aktueller und neuer gesetzlicher Risiko- und Compliance-Verpflichtungen zeugen von diesem Engagement. Zscaler bietet transparente Informationen und Support auf der Grundlage von Best Practices, damit Deployment und Verwaltung von Zscaler-Lösungen stets dem Governance-Framework entsprechen.

Weitere Ressourcen zum Thema „Work-from-Anywhere“

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com