zscaler™

ZSCALER

WIE PHARMA-UNTERNEHMEN DAS VOLLE POTENZIAL DER CLOUD AUSSCHÖPFEN KÖNNEN

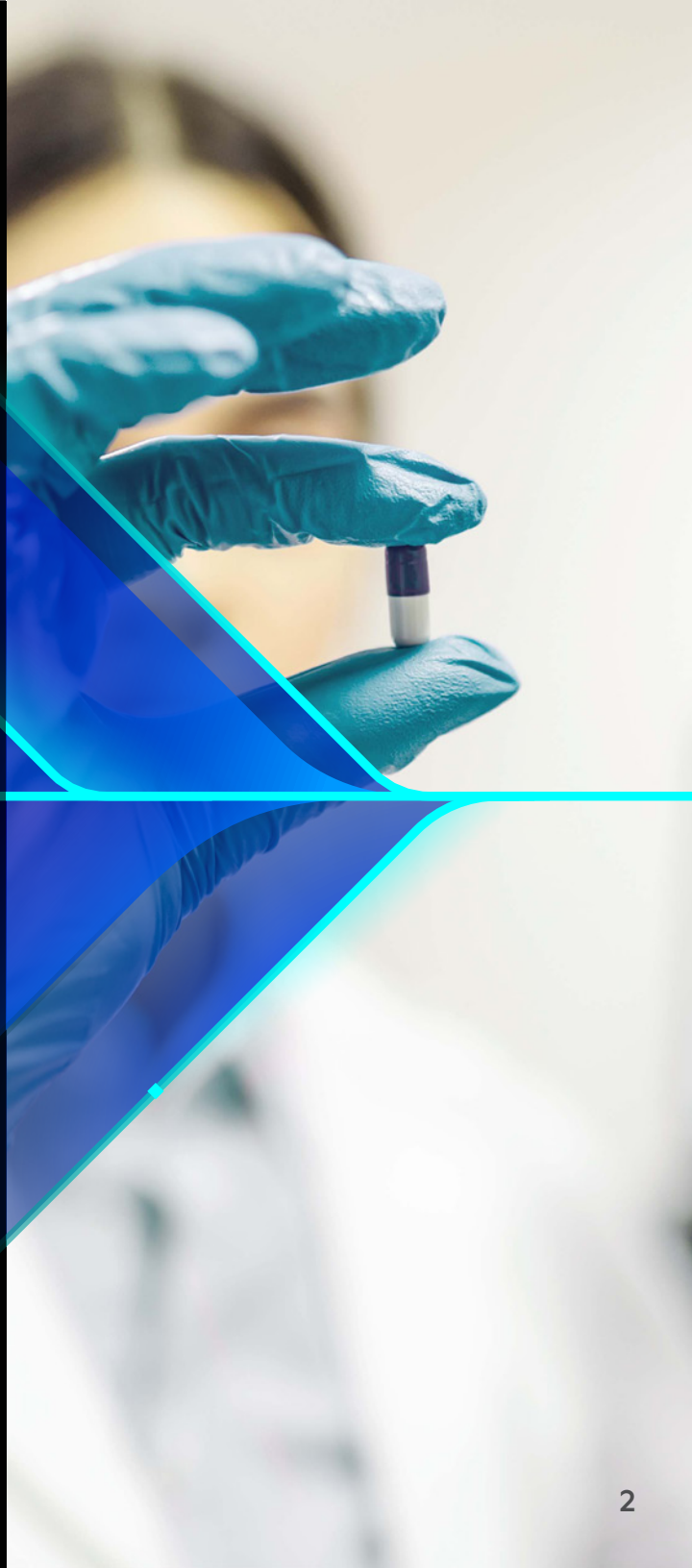
Mit Zero Trust und einer Cloud-basierten Security-Plattform die Wettbewerbsfähigkeit in der Pharmabranche erhalten und ausbauen

Möglichst früh mit Medikamenten, Impfstoffen oder anderen neuen pharmazeutischen Produkten an den Markt zu gehen, ist in der Pharmabranche heute oft überlebenswichtig. Pharmaunternehmen müssen Innovationen liefern, um sich im Wettbewerbsumfeld erfolgreich durchzusetzen und stehen daher nicht ohne Grund an der Spitze der Innovationskurve.

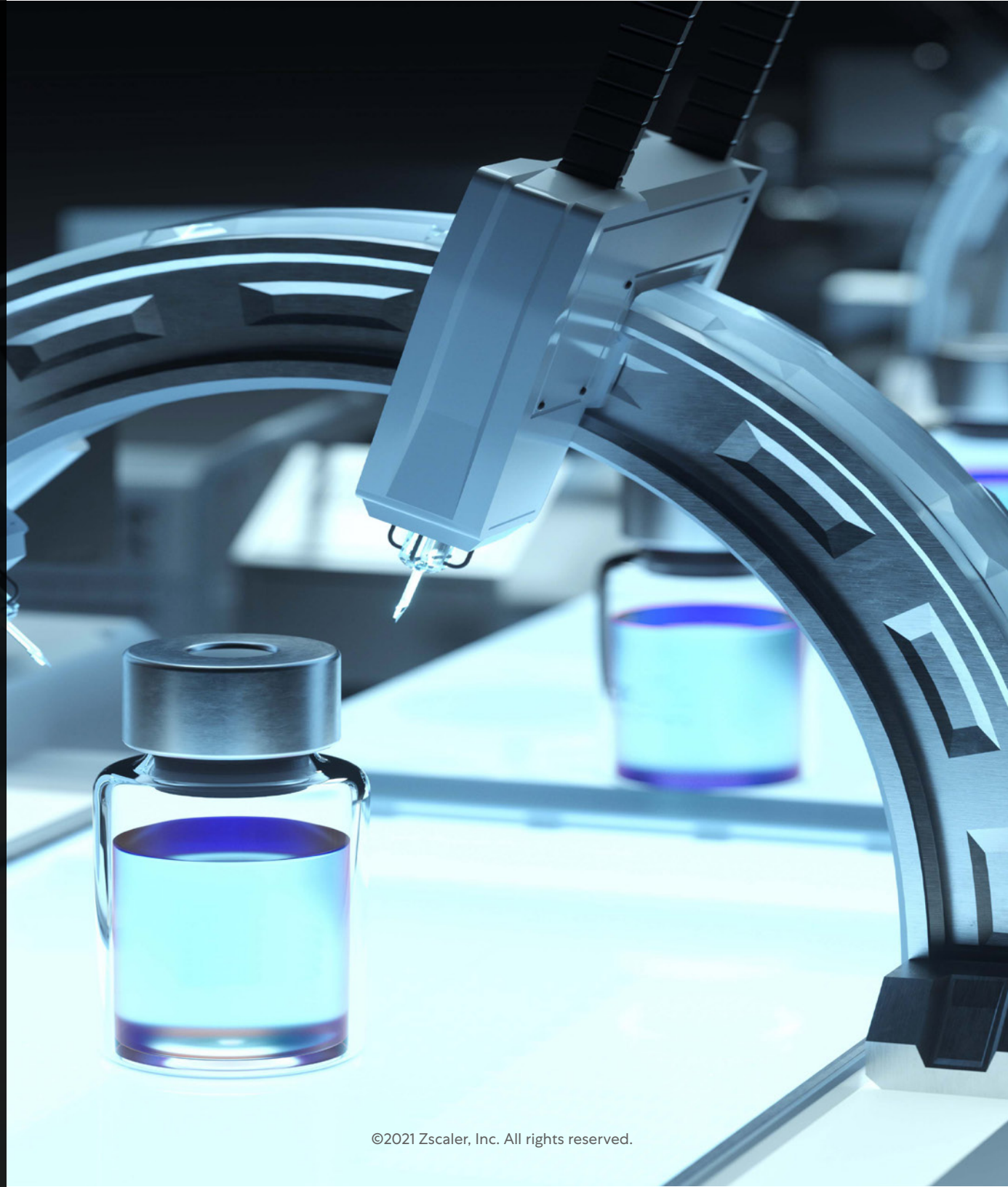
Auf der Suche nach Innovationsexzellenz, neuen Geschäftsmodellen und Wettbewerbsvorteilen gehen Pharmaunternehmen daher Kooperationsmodelle ein, die fest in der DNA der Branche verankert sind. Dabei kommt der Cloud eine nicht unerhebliche Rolle zu, denn sie ermöglicht Kollaborationen über die Unternehmensgrenzen hinweg. Zum einen sind es Partnerschaften mit externen Einrichtungen wie Kliniken, Laboren oder Forschungszentren, zum anderen investieren sie stark in Fusionen und Übernahmen. Denn durch Merger & Acquisitions (M&A) kann das Wachstum gesteigert, Innovationspotenzial schneller ausgeschöpft und zunehmenden regulatorischen Anforderungen besser standgehalten werden.

Aus solchen Kooperationsmodellen erwachsen jedoch auch komplexe IT-Infrastrukturen, die Pharmaunternehmen und deren IT-Abteilung vor neue Sicherheitsherausforderungen stellen. Besonders Marktführer des Pharma-Sektors sind unfreiwillig Cyber-Bedrohungen ausgesetzt. Die Kosten für den durch eine Sicherheitslücke entstandenen Schaden belaufen sich dabei auf durchschnittlich 5,06 Millionen US-Dollar. Damit liegt die Pharmaindustrie im Branchenvergleich an der Spitze.

Im Folgenden werden nun die mit den oben genannten Kollaborationsmodellen verbundenen technologischen Trends und die digitale Transformation hin zur Cloud beschrieben, ebenso wie die Herausforderungen, die sich daraus für die IT-Sicherheit von Pharmaunternehmen ergeben. Best-Practice-Beispiele zeigen auf, wie es Pharmaunternehmen gelingt, das volle Potenzial der Cloud auch in der IT-Sicherheit zu erschließen: indem ein Zero-Trust-Ansatz gewählt und dieser zugleich in einen Geschäftsvorteil verwandelt wird.



INHALT



1 NEUE **TECHNOLOGIE-TRENDS** AUF DEM VORMARSCH

Cloud-Technologien werden in Pharmaunternehmen immer stärker genutzt

Die digitale Transformation – also das Etablieren neuer Geschäftsmodelle auf Basis der Digitalisierung – wird mit dem Aufkommen neuer Technologien noch an Fahrt aufnehmen. Die Anzahl der Geräte und Netzwerke, die Pharmaunternehmen für ihre Geschäftsprozesse verwenden, wächst drastisch. Bereits heute werden Künstliche Intelligenz und maschinelles Lernen in Pharmaunternehmen in großem Umfang eingesetzt, um Big Data zu strukturieren. Das 5G-Netzwerk als infrastrukturelles Rückgrat für das Internet-of-Things ermöglicht es unzähligen Geräten innerhalb pharmazeutischer Produktionslinien, sich zu verbinden und mit hoher Geschwindigkeit zusammenzuarbeiten.

Der herkömmliche Rechenzentrumsbetrieb verliert heute an Bedeutung. Arbeitsprozesse werden mehr und mehr in die Cloud verlagert und Cloud-Technologien mit der bestehenden IT-Infrastruktur verbunden. Es ist also nicht mehr damit getan, das eigene Netzwerk mit einem sicheren Perimeter abzuschirmen. Herkömmliche Netzwerksicherheit war sinnvoll, solange alle Anwendungen im Rechenzentrum gehostet wurden und sich alle Nutzer im Netzwerk aufhielten. Auch die bisher verwendete Technik der Virtual Private Networks (VPN) wurde nicht dafür ersonnen, tausende Remote-Zugriffe zu managen, sie krankt an Latenz- und Sicherheitsproblemen.

Angesichts des schlagartig ansteigenden Home-Office-Betriebes ist es vielen Unternehmen zunächst gelungen, ihren Beschäftigten einen sicheren Cloud-basierten Fernzugriff auf das zentrale Unternehmensnetzwerk einzurichten. Der Anteil der von Zuhause aus Arbeitenden erhöhte sich aufgrund der Corona-Pandemie um das sechsfache und lag in Deutschland Anfang 2021 bei 24 Prozent. Allgemein wird prognostiziert, dass sich dieser Trend zur Remote Work in Zukunft verstärken wird und viele aus dem Home Office Arbeitende hybride Arbeitsmodelle bevorzugen werden. Gibt es unter diesen Bedingungen noch Bedarf für ein klassisches Büronetzwerk? Wie muss sich die IT-Infrastruktur adaptieren, um eine hybrid arbeitende Belegschaft dauerhaft unterstützen zu können?

2 WARUM **PHARMA-UNTERNEHMEN** JETZT HANDELN MÜSSEN

Kollaborationen als etablierte Pharma-Geschäftsmodelle

M&A sind für Pharmaunternehmen eine häufige Wachstumsstrategie, um der Konkurrenz einen Schritt voraus zu sein, neue Geschäftsmodelle und das dafür benötigte Know-how zu erschließen. Weltweit betrug 2018 das Transaktionsvolumen in der Pharmabranche knapp 150 Milliarden US-Dollar. Diese M&A-Aktivitäten müssen jedoch schnell umgesetzt werden, um Synergien zu beschleunigen und für eine rasche Monetarisierung zu sorgen. Genau hierbei erweist sich das zeitaufwändige Zusammenführen von Netzwerken als Hemmschuh für die Geschwindigkeit. Außerdem muss das gegenseitige Öffnen der Netzwerke abgesichert werden. So ziehen sich M&A-Aktivitäten oft Monate, teils sogar Jahre hin.

Eine permanente Herausforderung ist die Zusammenarbeit mit Drittanbietern. Diese müssen schnell und sicher auf die Kernsysteme zugreifen können, um eine effektive Partnerschaft zu ermöglichen. IT-Fachleuten fehlt aber meist die Transparenz darüber, wer unter welchen Sicherheitsparametern Zugang zu welchen Daten und Tools hat. Dadurch setzen sich Unternehmen unfreiwillig einem Sicherheitsrisiko aus. Wie kann die IT-Abteilung kontrollieren, mit welchen Drittparteien das Unternehmen zusammenarbeitet, wie kann sie sicherstellen, dass der Zugriff nur auf benötigte Apps erlaubt wird, ohne das gesamte Netzwerk zu tangieren? Es gibt eine Reihe regulatorischer Bedenken beim Arbeiten in der Cloud, insbesondere was die Zusammenarbeit mit Partnern angeht. Alle Arbeitsumgebungen müssen verifiziert und Informationen vor unberechtigtem Zugriff geschützt werden.

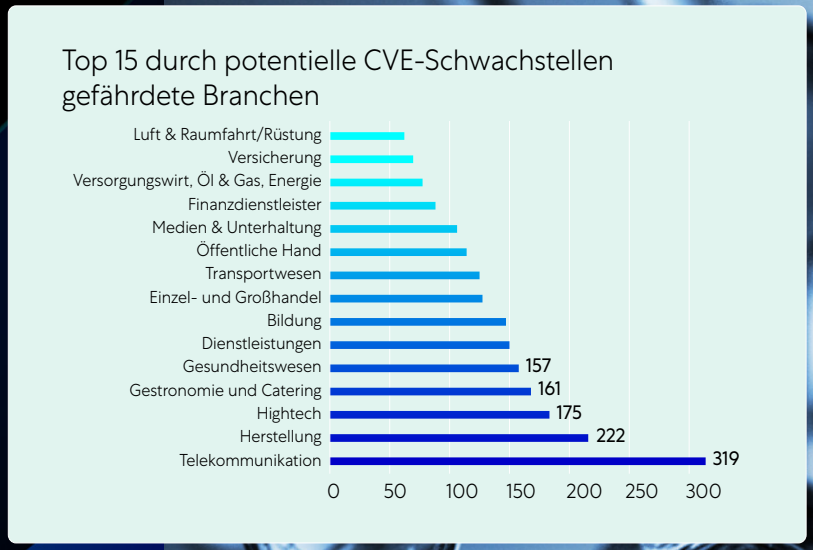
Auch die Produktion in China stellt die Branche vor zusätzliche Hürden. Das Reich der Mitte schottet sich stark vom World Wide Web ab. Elektronische Geschäftskorrespondenz wird durch die große China-Firewall erheblich verlangsamt, wenn nicht sogar blockiert. Pharmaunternehmen, die heute wie selbstverständlich Google-Dienste nutzen, erschwert dies eine reibungslose Geschäftsabwicklung mit ihren chinesischen Produktionsstandorten. Von mobilen Arbeitsplätzen oder vom Home Office aus aber wird es kompliziert, sich zu verbinden.

Veraltete IT und erhöhte Netzwerkkomplexität

Die großen global tätigen Pharmaunternehmen haben in den Jahrzehnten ihres Bestehens unzählige Geschäftsmodelle durchlaufen, neue eingeführt aber auch hinter sich gelassen. Daraus erwuchs mit der Zeit eine komplexe, oft schwer überschaubare IT-Umgebung, die es zu verwalten gilt, einschließlich der damit verbundenen Sicherheitsfragen.

Auf der Suche nach schnellen Lösungen haben viele Beschäftigte eigenständig Lösungen an der IT vorbei installiert und eine sogenannte Schatten-IT geschaffen, die sich somit einer zentralen Kontrolle entziehen.

Erschwerend kommt der weltweit herrschende Mangel an qualifizierten Sicherheitsfachkräften, die sich der Security-Aspekte im bestehenden Netzwerk annehmen könnten, hinzu. Ein Drittel der deutschen Unternehmen geben an, Probleme bei der Suche nach IT-Fachkräften zu haben. Und so dauert es durchschnittlich sechs Monate, bis eine IT-Stelle besetzt werden kann. War der Fachkräftemangel schon vor der Pandemie ein Problem, hat sich der Kampf um Talente angesichts der ausufernden Aufgaben zur Verwaltung komplexer IT-Umgebungen nochmals verschärft.



Erhöhte Cyberkriminalität durch zunehmende Digitalisierung

Mit der Digitalisierung öffnen sich zahlreiche Sicherheitslücken, die eine permanente potenzielle Bedrohung für alle Wirtschaftsbereiche darstellen. Nicht nur Digitalisierungstechnologien entwickeln sich rasant weiter, auch die Methoden und Instrumente der Cyberkriminellen werden immer ausgefeilter. Die Pharma- und Gesundheitsindustrie gehört dabei zu den besonders ins Visier genommenen Branchen, davon zeugen zahlreiche bekannt gewordene Beispiele der jüngeren Vergangenheit.

Die Folgen für die Unternehmen sind Verlust von Markenreputation und Intellectual Property, verzögerte Markteinführungszeit und hohe Kosten zur Abwehr bzw. Beseitigung von Schäden.

Fazit

Die Modernisierung der IT ist für Pharmaunternehmen weniger eine Option denn vielmehr eine Dringlichkeit, um Cyber-Angriffen vorzubeugen. Ein Zero-Trust-Sicherheitskonzept schützt nicht nur vor Sicherheitslücken, sondern sollte Bestandteil einer ganzheitlichen Transformationsstrategie sein, um die Innovationskraft in der Pharmabranche zu stärken.

Erfahren Sie mehr über Cyberkriminalität

3 WIE ZERO TRUST DIE HÜRDEN DER IT-SICHERHEIT ÜBERWINDEN KANN

Zero Trust

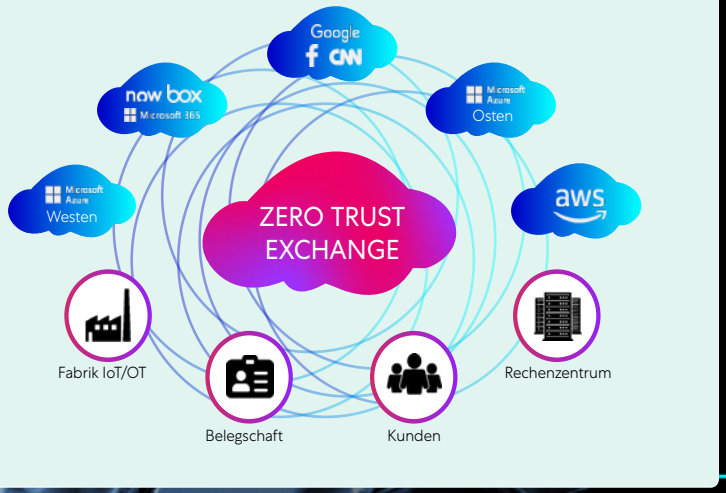
ist ein ganzheitlicher Ansatz zur Sicherung von Unternehmen im Zeitalter der Digitalisierung. Er beruht auf dem Prinzip der minimalen Zugriffsrechte sowie dem Grundsatz, dass kein User oder keine Anwendung inhärent als vertrauenswürdig gelten darf. Entsprechend wird Vertrauen nur basierend auf der Benutzeridentität und dem Kontext aufgebaut, wobei Richtlinien bei jedem Schritt als Gatekeeper dienen.

Pharma-Unternehmen müssen sich darauf einstellen, ihre Abwehr- und Kontrollmechanismen dort einzurichten, wo Verbindungen hergestellt werden: im Internet. Damit diese schnell und sicher sind, unabhängig davon, wie oder wo sich Nutzer verbinden und auf ihre Anwendungen zugreifen, braucht es ein neues Konzept: den sogenannten Zero-Trust-Ansatz.

Das Zero-Trust-Sicherheitskonzept basiert auf dem Grundsatz, keinem Gerät, Nutzer oder Dienst innerhalb oder außerhalb des eigenen Netzwerks von vornherein zu vertrauen. Um es umzusetzen, sind umfangreiche Maßnahmen zur Authentifizierung sowie zur Prüfung des Netzwerkverkehrs zu treffen. Das Risiko für Firmennetze und -anwendungen wird minimiert, indem Sichtbarkeit für den gesamten Datenverkehr hergestellt wird und richtlinienbasierte Zugriffsrechte auf das Internet und Applikationen in Multicloud-Umgebungen oder das Rechenzentrum vergeben werden.

Durch Einführung einer Cloud-basierten **Zero-Trust-Security-Plattform** können Pharmaunternehmen ihre aktuellen IT-Problemstellungen lösen. Es handelt sich dabei um eine ganzheitliche Umstrukturierung, bei der Apps, Security-Aspekte, Konnektivität und eine neue Netzwerkarchitektur miteinander verbunden werden. Auf dieser Basis können Unternehmen ihre digitale Transformation strategisch angehen.

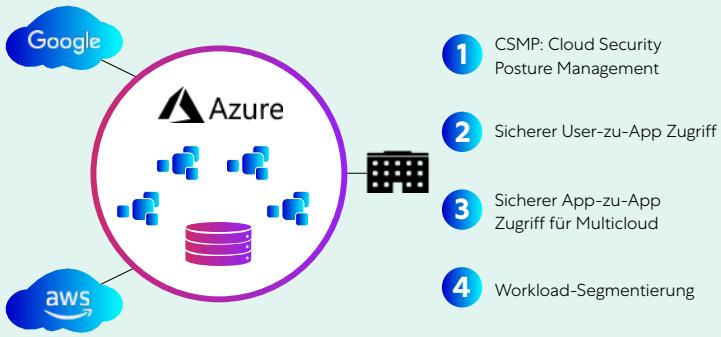
Erfahren Sie mehr über
Zscaler Zero Trust Exchange



Netzwerk-Komplexität in Multicloud-Umgebungen

Die Zero Trust Exchange Plattform von Zscaler ermöglicht es Beschäftigten mit schnellen und sicheren Verbindungen, von überall auf Anwendungen zuzugreifen, sodass das Internet effektiv als Unternehmensnetzwerk fungiert. Der Zugriff einzelner Nutzer wird granular auf Ebene der Anwendung segmentiert: Remote-Zugriff zum Rechenzentrum ebenso wie für Anwendungen in Cloud-Umgebungen. Der Zero Trust Exchange schützt Tausende von Kunden vor Cyberangriffen und Datenverlusten, indem sie Benutzer, Geräte und Anwendungen von jedem Standort aus sicher auf Basis von Richtlinien über einen verschlüsselten Microtunnel verbindet.

Die vier Kerneigenschaften von ZCP



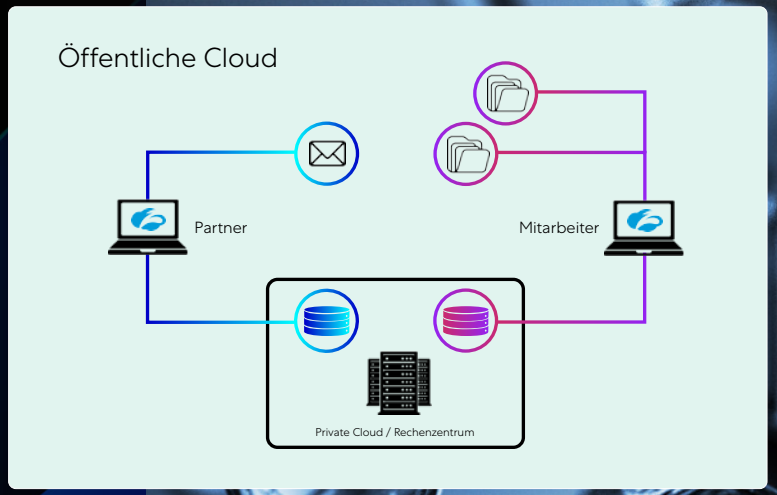
Zscaler Cloud Protection (ZCP) nutzt die Zero Trust Exchange-Plattform von Zscaler und mindert nicht nur das mit der Cloud-Migration verbundene Risiko, sondern auch die operative Komplexität. ZCP identifiziert Workloads in der Cloud und gewährleistet eine starke Security Posture, ermöglicht sicheren Anwendungszugriff ausschließlich für befugte User und sicheren Zugriff für Workloads auf andere Clouds, Rechenzentren und das Internet. Zudem zielt sie auf die Minderung von Angriffsrisiken durch Verhinderung lateraler Bewegungen von Angreifern ab.

Anwenderinnen und Anwender erwarten schnelle, nahtlose digitale Erlebnisse, die die Zscaler Zero Trust Exchange unterstützt. Die Messung und Verbesserung digitaler Erlebnisse in einer Cloud- und Hybrid-Arbeitswelt erfordert eine einheitliche Sicht auf die Leistungsmetriken von Anwendungen, CloudPath und Endpunkten. Zscaler Digital Experience ist ein Cloud-nativer Service, der als Teil der weltweit größten Sicherheits-Cloud Probleme der Benutzererfahrung analysiert, behebt und löst.

Erfahren Sie mehr über
Zscaler Cloud Protection

Sicherheit

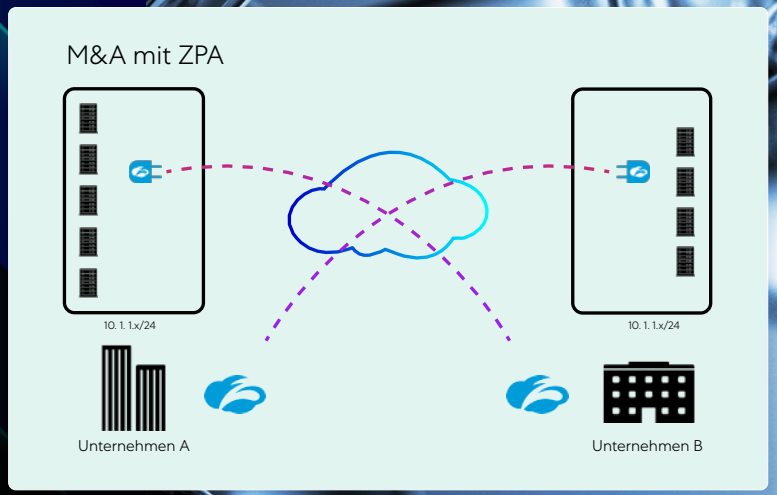
Der Übergang von einer starren, auf einen Perimeter fixierten Sicherheitsarchitektur zu einem Konzept, das unterschiedlichen Architekturen und Kontrollpunkten in der Cloud gerecht wird, erfordert sowohl theoretische als auch praktische Änderungen. Hierfür bedarf es eines neuen Denkansatzes bezüglich einer Lösung sowie der passenden Technologie für deren Implementierung. Die Sicherheit selbst muss in die Cloud verlagert werden. Die Cloud und Zero-Trust schaffen die Voraussetzungen für eine Komplettlösung. Dies ist der Kern des Zero-Trust-Ansatzes für eine sichere Cloud-Transformation.



Merger & Acquisitions

Jedes Jahr werden mehr als 50.000 Fusionen, Übernahmen und Veräußerungen abgewickelt. Das Zusammenführen von Netzwerken erweist sich dabei häufig als extrem zeitaufwändig. Ein Cloud-basiertes Sicherheitskonzept vereinfacht nicht nur die IT-Integration während M&As oder Veräußerungen und verkürzt den Prozess auf wenige Wochen, sondern verringert auch die Angriffsfläche des Unternehmens.

Zscaler Private Access (ZPA) ist eine Cloud-basierte Lösung, die über die Zscaler Zero Trust Exchange sicheren Zugriff zu internen Anwendungen bereitstellt, die in der Cloud oder einem Rechenzentrum gehosted werden. Durch die Vergabe von granularen Zugriffsberechtigungen kann ZPA berechtigten Mitarbeitern auch bei Firmenübernahmen den Zugang zu den benötigten Applikationen im übernommenen Netzwerk gewährleisten – ohne das gesamte Netzwerk für den Zugriff zu öffnen.



Erfahren Sie mehr über Zero Trust in der Cloud

Erfahren Sie mehr über Zscaler Private Access (ZPA)

Mike Towers

CISO bei Takeda

> Insgesamt haben der Mehrwert für unser Unternehmen und die Ergebnisse durch unsere Parnerschaft mit Zscaler und unser Weg zu Zero Trust uns eine kürzere Zeitspanne bis zur Wertschöpfung ermöglicht.

4 IT-TRANSFORMATION VORANTREIBEN – MIT **ZERO TRUST**

IT-Verantwortliche in Pharma-Unternehmen bewerten den Einsatz neuer Cloud-basierter Technologien aus einer technisch-strategischen Brille heraus. Ihnen geht es insbesondere darum, die digitale Transformation des eigenen Unternehmens voranzutreiben.

Die digitale Transformation strategisch umsetzen

Eine Strategie zur Umsetzung der digitalen Transformation ist insbesondere in schnelllebigen und hochkompetitiven Märkten wie der Pharmabranche wichtig, um bisherige Wettbewerbsvorteile zu halten und auszubauen. Hier wird an den drei Säulen Cyber Security, IT-Transformation und User Experience angesetzt.

Cyber Security, das bedeutet, den sicheren Betrieb von Anwendungen und Netzwerk sicherzustellen, vor Ort ebenso wie remote. Präventiv muss nach Sicherheitslücken gesucht werden, um diese schnellstmöglich zu schließen. Dies gilt insbesondere bei der Integration von IT-Infrastrukturen im Zuge von M&A-Aktivitäten. App/Network Segmentation und Zugriffsbeschränkung (z. B. bei der Impfstoffentwicklung) sind dafür die geeigneten Instrumente. Sie minimieren laterale Bewegungen im Netzwerk und sichern die Zusammenarbeit mit Externen, indem sie ihnen möglichst wenig privilegierten Zugriff gewähren.

Bei der **IT-Transformation** geht es darum, die Komplexität der Infrastruktur (die im Zuge von M&A-Aktivitäten grundsätzlich zunimmt) zu reduzieren. Unternehmenszusammenschlüsse müssen technisch umgesetzt werden. Legacy-Systeme müssen abgelöst und die Business Operations beschleunigt werden, indem man auf moderne Cloud-basierte Tools umsteigt.

Den Beschäftigten zu ermöglichen, zuverlässig von überall aus arbeiten zu können (Remote Work), unabhängig vom Endgerät bei stets gleichbleibend guter Performance – dies steht im Mittelpunkt einer Optimierung der User Experience. Ein hohes Sicherheitsniveau darf dabei nicht im Widerspruch zur Produktivität am Arbeitsplatz stehen.

5 SICHERES GESCHÄFTS-WACHSTUM STÄRKEN – MIT **ZERO TRUST**

Geschäftsverantwortliche wollen durch die Umsetzung einer Zero-Trust-Strategie über eine Cloud-basierte Security-Plattform vor allem die Innovationskraft ihres Unternehmens stärken, Wachstum und Profitabilität sichern sowie eine schnelle Monetarisierung von M&A- und R&D-Aktivitäten erreichen.

Die Innovationskraft ausschöpfen

Um in dem hoch kompetitiven Marktumfeld des Pharmasektors wettbewerbsfähig zu bleiben, sind Innovationsfähigkeit, Prozesseffizienz und -sicherheit sowie eine kurze Time-to-Market unerlässlich. Die richtige Auswahl und der Einsatz geeigneter Technologien unterstützen Geschäftsentscheider darin, diese strategischen Ziele zu erreichen. Dabei wird an den drei Teilbereichen Wachstum und Entwicklung, reduziertes Geschäftsrisiko und Operational Excellence angesetzt.

Wachstum und Entwicklung, das bedeutet: M&A-Aktivitäten werden beschleunigt und damit schnell monetarisiert sowie Markteinführungszeiten reduziert (Impfstoffentwicklung!). Eine moderne IT-Infrastruktur hilft dabei, das Innovationspotenzial bestmöglich auszuschöpfen und die Zusammenarbeit mit Partnern in allen Bereichen zu verbessern. Sie unterstützt außerdem bei der Implementierung neuer Erlösmodelle und angepasster Lieferketten.

Im Bereich **reduziertes Geschäftsrisiko** geht es darum, Sicherheitsrisiken bei gleichzeitigem Trend hin zum mobilen Arbeiten zu minimieren und dadurch den Schutz der wertvollsten Vermögenswerte zu gewährleisten. Denn durch vermehrte Home-Office-Modelle, die Zusammenarbeit mit externen Parteien und auch die Integration im Zuge von M&A hat die Gefahr von potenziellen Cyber-Bedrohungen sichtlich zugenommen.

Operational Excellence bedeutet, Produktivität und Effizienz zu optimieren, um Innovationen zu beschleunigen. Schnelle Monetarisierung und eine kürzest mögliche Time-to-Market für neue pharmazeutischen Produkte sind auch hier die kritischen Faktoren.

6 DIE ZENTRALEN VORTEILE MIT **ZSCALER**

Mit Zscaler, dem First Mover bei der sicheren digitalen Transformation in der Pharmaindustrie, haben Unternehmen der Pharmabranche einen erfahrenen Experten an der Seite. Durch Einsatz der weltweit größten Zero-Trust-Exchange-Plattform mit ihrer Zero-Trust-Proxy-Architektur stärken Pharma-Unter-nehmen ihre Innovationskraft. Sie versetzen sich in die Lage, das Projekt „Digitale Transformation“ mit höchster Wertschöpfung und minimierten Risiken anzugehen.

- **Architektur**: Bestehende Architekturen werden überlagert, um die digitale Transformation zu beschleunigen und effiziente, sichere, kundenorientierte und skalierbare Services bereitzustellen.
- **Effizienz**: Eine vereinfachte IT reduziert Komplexität und Kosten.
- **Sicherheit**: Verbesserte Ausfallsicherheit und eine insgesamt höhere Sicherheitslage durch ein zentrales, abteilungsübergreifendes Monitoring verhindert Datenverluste und minimiert Sicherheitsrisiken
- **Kundenorientierung**: Ein Zero-Trust-Sicherheitskonzept unterstützt Work-from-anywhere-Umgebungen, erhöht Kapazitäten, reduziert Latenzen und schafft eine konsistente Benutzererfahrung.
- **Skalierbarkeit**: Eine moderne, agile Plattform untermauert digitale Innovationen, beschleunigt die digitale Transformation und schafft Kapazitäten für Wachstum.
- **M&A-Aktivitäten**: Diese stellen eine Herausforderung für Netzwerk- und Sicherheitsteams dar, die dafür verantwortlich sind, die Konnektivität der Benutzer zu internen Apps und die Sicherheit sensibler Daten zu gewährleisten. Eine Zero-Trust-Plattform sorgt hier für Sicherheit und eine schnellere Monetarisierung von Fusionen und Akquisitionen.

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