

Gewährleisten von Business Continuity in der Cloud: Wie das Unternehmen Takeda Pharmaceuticals den Remote Access skalierte



Auszug aus *Absicherung von Remote-Arbeit – Gewährleistung von Business Continuity mit Zscaler™* © 2020, alle Rechte vorbehalten.



Company Background

Unternehmen:	Takeda Pharmaceutical
Branche:	Pharmazie
Verantwortlicher:	Mike Towers
Rolle:	CISO
Umsatz:	32 Mrd. USD
Mitarbeiter:	52.000
Länder:	110
Standorte:	575

IT-Footprint des Unternehmens

Takeda Pharmaceutical mit Sitz in Tokio ist das älteste Pharmaunternehmen der Welt. Durch die Übernahme von Shire PLC im Jahr 2019 wurde seine Präsenz auf mehr als sechzig Büro- und Forschungsstandorte weltweit ausgeweitet. Das IT-Team von Takeda verwaltet die Systeme für die mehr als 70.000 weltweite Mitarbeiter von Cambridge, Massachusetts, aus.

„ Wir verwenden eine Art von App-zu-App-Ansatz, um den Leuten das zu geben, was sie brauchen, ohne ihnen unbegrenzten Zugang zu gewähren. Dank der Kombination aus ZIA und ZPA sind wir viel flexibler in Bezug auf das, was wir bereitstellen, und da wir unseren gesamten Traffic darüber laufen lassen, wissen wir, dass das System skalierbar ist.“

Mike Towers, Chief Information Security Officer, Takeda Pharmaceutical Company

Für CISO Mike Towers war es eine Fusion – eine sehr große Fusion –, die die sichere Cloud-Transformation von Takeda Pharmaceutical forcierte.

„Wir haben Shire PLC im Januar 2019 übernommen und damit die Größe des Unternehmens verdoppelt“, erklärt Towers. Durch die Übernahme von Shire vergrößerte sich die Belegschaft von Takeda erheblich. Towers stand vor der Aufgabe, ein inkongruentes Patchwork von Netzwerk- Hardware-Technologien integrieren zu müssen.

Hilfe aus der Cloud für ein „zergliedertes“ Netzwerk

Zum Glück für seinen CISO hatte Takeda Ende 2018 mit der Einführung von Zscaler Internet Access (ZIA) begonnen, hauptsächlich, um den Internetzugang der Mitarbeiter über die Cloud abzusichern und Benutzern an jedem beliebigen Ort und auf jedem

verwendeten Gerät eine konsistentere Erfahrung zu vermitteln. Doch ZIA erwies sich als besonders wertvoll, als Towers und sein Team mit der Integration einer, wie er es nennt, „ziemlich zergliederten“ Netzwerkarchitektur konfrontiert waren.

„Wir hatten etwa 320 Firewalls, die über lokale Standorte, regionale Standorte, Kernstandorte und so weiter verteilt waren“, sagt Towers. „Es war eine sehr, sehr traditionelle, auf Appliances basierte On-Premise-Netzwerkarchitektur. Das war die vorherrschende Art und Weise, wie der Perimeter und das Netzwerkdesign konzipiert, entwickelt und eingesetzt waren.“

Die Fusion beschleunigte Takedas Migration in die Cloud: „Wir waren bereit, uns auf ein Zero-Trust-, Benutzer-zu-Ziel-Modell umzustellen“, fährt Towers fort. „Wir wollten so schnell wie möglich realisieren

und haben mittels ZIA standardisiert. Auf diese Weise können wir unsere 'Next-Generation' Firewalls ersetzen.“

ZIA gab Towers und Takeda größere Flexibilität bei der Einrichtung einer sicheren Mitarbeiterkonnektivität – für jede Art von Beschäftigten – über lokale Internet-Breakouts. Towers weist darauf hin, dass die auf Richtlinien basierten Verwaltungskontrollen von Zscaler dazu beitrugen, Takeda agiler zu machen: „70.000 Mitarbeiter in 110 Ländern, aber nur eine Richtlinie“, erklärt er. „Wir können unabhängig davon, wo Benutzer hinreisen, dieselbe Richtlinie anwenden mit derselben konsistenten Erfahrung vor Ort und außerhalb des Netzwerks. Wenn man vor der Herausforderung steht, sowohl die Nutzererfahrung als auch die Sicherheit zu verbessern, kann man das mit Zscaler schaffen, weil die Leute flexibel sein können.“

Bereitstellung von ZPA, zuerst langsam... dann sehr, sehr schnell

In einer Industrie, die auf Forschung aufbaut, ist Takeda Pharmaceutical in hohem Maße von der internen Entwicklung abhängig und die erfordert einen umfangreichen Einsatz von proprietären Technologien, Anwendungen und geistigem Eigentum. In der Vergangenheit hatte diese Abhängigkeit Takedas Migration in die Cloud verlangsamt.

Im Hinblick auf die Cloud-Zukunft wünschte sich Towers „ein Modell des Remote Access für Anwendungen, die sich traditionell im Rechenzentrum befinden“. Er verweist auf Zwänge durch Vorschriften und „Maschinennähe“ als Grund dafür, Ressourcen vor Ort zu behalten: „Bei einer Produktionsanlage oder einem F&E-Labor gibt es teure Geräte in diesem Umfeld, die per Computer betrieben werden müssen. Diese müssen oft vor Ort bleiben, und wir möchten, dass Mitarbeiter auf die dortigen Anwendungen zugreifen können, ohne Zugang zum gesamten Netzwerk zu erhalten.“

2019 begannen Towers und sein Team mit der Einführung von Zscaler Private Access (ZPA), um eine sichere Konnektivität zu internen Ressourcen bereitzustellen, wobei das Deployment sowohl nach Anwendung als auch nach Benutzer priorisiert wird. Towers merkt an, dass das in Tokio ansässige Takeda – das älteste Pharmaunternehmen der Welt – „werteorientiert“ sei und der Wechsel zu ZPA eine Art kultureller Wandel für das Unternehmen gewesen sei.

Towers konzentrierte sich zunächst auf die Erweiterung des Remote Access und die Stilllegung von VPN-Hardware. „Remote Access bedeutete früher immer Fernzugriff auf das Netzwerk“, sagt Towers. „Aber so denken wir nicht mehr.“ ZPA veränderte die Denkweise von Towers hinsichtlich der VPN-Technologie bei Takeda: „Remote-Benutzer sind es gewohnt, auf einen VPN-Klienten zu klicken, um eine Verbindung herzustellen, aber bei VPN geht es nicht um Anwendungszugriff sondern um Netzwerkzugriff. Uns ging es mehr um die Anwendungen und Dienste, die Mitarbeiter benötigen... und VPN bringt da nicht viel, weil man in ein Netzwerk gelangt, nur um es gleich wieder zu verlassen.“

Towers musste die Infrastruktur von Takeda neu bewerten, insbesondere die weitere Nutzung von VPN-Technologie im Hinblick auf Takedas Fortschritte bei der Cloud-Transformation.

Wenn er heute an VPNs denkt, fragt Towers rhetorisch: „Wozu?“ Und er ergänzt: „Das gleiche Maß an Sicherheit und Kontrolle können wir auch in der Cloud bereitstellen. Wir wollen so viel Reibung wie möglich beseitigen.“ Zscaler ist Takeda bei der Beseitigung dieser Reibung behilflich. Towers fährt fort: „ZPA ermöglicht den Zugriff auf Anwendungen, ohne dass sich jemand Gedanken darüber machen muss, ob er auf ein anderes Fenster oder eine Emulationsmaschine klicken muss, um Zugang zu erhalten... Wir wollen diese Fähigkeit so schnell und reibungslos wie möglich unterstützen.“

Wenn das Arbeiten im Homeoffice zur neuen Normalität wird

Anfang 2020 waren Towers und sein Team mit der schrittweisen Einführung von ZPA bei Takeda beschäftigt. Und dann passierte der Ausbruch des Coronavirus. Wie viele internationale Firmen erlebte auch Takeda seine ersten Betriebsstörungen in China, wo die Niederlassungen laut Towers immer noch „veraltete VPN-Infrastrukturen mit „überholten Netzwerkarchitekturen“ verwendeten, „die den Zugriff auf Anwendungen und die Leistung ziemlich verlangsamten.“ Die Lösung? Eine „schnelle Umstellung auf ZPA“ unter der Leitung von Towers und seinem Team.

Als der dringende Bedarf an Remote Access für Mitarbeiter stieg, musste Towers herausfinden, wie er und seine Kollegen rund um den Globus angesichts solcher „beispiellosen“ Herausforderungen die Business Continuity aufrechterhalten konnten. „Wir hatten noch nie eine Situation, in der so viele Menschen von zu Hause aus arbeiten“, sagt er. „Man übt zwar regelmäßig für ein weit verbreitetes Arbeiten im Homeoffice, aber niemand übt mit allen zur gleichen Zeit und wenn alle Kinder und Familien zu Hause sind.“ Zugang war eine Sache, die Verwaltung von überlasteter Bandbreite eine ganz andere: „Jeder Mitarbeiter [zu Hause] konkurriert mit Netflix und Xbox, die von den Kindern zur gleichen Zeit genutzt werden. Deshalb mussten wir uns auf die Optimierung des Internetzugangs konzentrieren.“

Towers und sein Team untersuchten, wie Takeda-Benutzer mit internen Anwendungen arbeiten. Sie verschoben Takedas „Kontroll- und Bereitstellungsansatz“, sodass sich die Benutzer damit befassen konnten, welche Anwendungen sie zum Erledigen ihrer Arbeit benötigten, und nicht so sehr damit, wo sich diese Anwendungen befanden. „Wir wollen nicht mehr so denken“, erklärt er,

und jetzt kann die IT stattdessen „eine Art App-by-App-Ansatz bereitstellen, um Mitarbeiter auf das zugreifen zu lassen, was sie benötigen, ohne ihnen zu viele Zugangsrechte zu geben.“



Abbildung 6-3. CISO Mike Towers leitete Takedas (beschleunigte) Initiative, um den Beschäftigten das Arbeiten von überall aus zu ermöglichen. Er stellte vier Ziele in den Vordergrund: Remote Access, VPN-Ersatz, bessere Nutzererfahrung und Kontrolle (unabhängig davon, ob das System vor Ort oder in der Cloud ausgeführt wird).

Wenn Remote-Arbeit nicht mehr, sondern weniger Hardware bedeutet

ZPA ermöglichte es Towers und seinem Team, die Umstellung von Takeda auf den vollständigen Remote-Betrieb abzusichern. Durch die Einführung von ZIA und ZPA erreichte Takeda, was Towers als „erhebliche Kostenersparnisse“ bezeichnet, da die Firewall-Hardware stillgelegt werden konnte. CISO Towers beabsichtigt, die Zahl der

Firewall-Appliances des Unternehmens von der ursprünglichen Höchstmenge (über 320!) auf nur noch ein Dutzend zu senken.

Die von Takeda mit Zscaler realisierten Vorteile beschränken sich nicht auf VPN und Firewall-Hardware. Nachdem Towers mit „einer Menge Nischen-Punktlösungen“ zu kämpfen hatte, nutzt er nun die Funktionen des Cloud Access Service Broker (CASB) über die Inline-Proxy-Sicherheitsarchitektur: „Zscaler unterstützt uns dabei, mit CASB-Kontrollen mehr zu erreichen“, erklärt Towers, „nämlich intelligenter mit Daten umzugehen und auf Daten gestützte Sicherheitsentscheidungen zu treffen. Und da es ein Cloud-Service ist und wir bereits unseren Traffic durchleiten, wissen wir, dass er skalierbar [und] operativ stabil ist.“

Da Mitarbeiter auf lokale Internet-Breakouts umgestiegen sind, konnte Towers kostspielige Netzwerke stilllegen. „98 Prozent dessen, worauf [Benutzer] zugreifen, befindet sich ohnehin im Internet“, erklärt er. „Wir können eine Menge teurer WAN-Verbindungen loswerden.“

In den letzten beiden Jahren mussten Towers und sein IT-Team (viel geschickter als sie es sich hätten vorstellen können) operative Hürden überwinden, die sich ihnen in den Weg stellten. Doch obwohl die sichere Cloud-Transformation seines Unternehmens schneller voranschreitet als geplant, bleibt Towers optimistisch.

„Dank der Kombination aus ZIA und ZPA sind wir viel flexibler in Bezug auf das, was wir bereitstellen können, und da wir unseren gesamten Traffic darüber laufen lassen, wissen wir, dass das System skalierbar ist,“ schließt Towers. „Dies sind gute Zeiten für Sicherheitsexperten, denn man braucht sich keine Gedanken mehr darüber machen, wie man Nutzererfahrung und Sicherheit vereinbart. Man kann beides erreichen!“



Über Zscaler

Zscaler wurde im Jahr 2007 auf der Grundlage eines einfachen aber wirkungsvollen Konzepts gegründet: Da Anwendungen in die Cloud verlagert werden, muss sich auch die Sicherheit dorthin bewegen. Heute helfen wir Tausenden von globalen Organisationen bei der Transformation zu Cloud-fähigen Betriebsabläufen.

© 2021 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™ ist entweder (i) eine eingetragene Handelsmarke oder Dienstleistungsmarke oder (ii) eine Handelsmarke oder Dienstleistungsmarke von Zscaler, Inc. in den Vereinigten Staaten und/oder anderen Ländern. Alle anderen Markenzeichen sind Eigentum ihrer jeweiligen Besitzer.