

Zscaler™ ermöglicht MAN Energy Solutions die Transformation von Netzwerk und Anwendungen

MAN Energy Solutions mit Sitz in Augsburg, Deutschland, ist der weltgrößte Anbieter von Großdieselmotoren und Turbomaschinen für Schiffe und stationäre Verwendung. Das Unternehmen entwickelt Zweitakt- und Viertaktmotoren, die sowohl im eigenen Werk als auch von Lizenznehmern hergestellt werden. MAN Energy Solutions entwickelt und produziert auch Gasturbinen. Abgerundet wird die Produktpalette durch Turbolader, Propeller, Gasmotoren und Chemiereaktoren.

Herausforderung

Während das Geschäft weltweit wächst, vollziehen sich rapide Technologieänderungen wie IoT für Motoren und Systeme jeder Größenordnung, die rund um den Globus im Transportwesen eingesetzt werden. Gleichzeitig arbeitet eine große, international verteilte Belegschaft zunehmend mobil und muss **mobilen Zugang** zu Web-Applikationen und spezifischen Geschäftsanwendungen erhalten.

Der traditionelle Ansatz von Festung-mit-Burggraben für die Netzwerk- und Applikations-**Sicherheit** passt nicht mehr zu modernen Cloud-Deployments, die globale Skalierung, globalen Zugang und eine verbesserte Sicherheitslage möglich gemacht haben, als Workloads zu AWS und Azure migrierten und das Internet zum neuen Unternehmensnetzwerk wurde. Jetzt gilt es, diese Anwendungen für das Internet unsichtbar zu machen und authentifizierten Zugang nur zwischen vertrauenswürdigen Benutzern und vertrauenswürdigen Anwendungen zuzulassen.

MAN Energy Solutions stellte fest, dass die erhöhte **Geschwindigkeit und Agilität** des Cloud-Deployment durch eine schlechte Nutzererfahrung



MAN Energy Solutions

man-es.com

Standort: Augsburg, Deutschland

Branche: Herstellungs- und Transportdienste

Benutzerzahl: 12.000 Benutzer an über 100 Standorten in 70 Ländern

Zscaler Produkte: Zscaler Private Access (ZPA), Zscaler Internet Access (ZIA)

„Angesichts der zunehmenden Nutzung von Mobilitäts- und Cloud-Diensten wandelt sich die IT-Landschaft. Unternehmen müssen ihre IT-Architektur ändern, um dem wachsenden Bedarf an Sicherheit für Benutzer an jedem Ort und auf jedem Gerät gerecht zu werden.“

– Tony Fergusson
IT-Infrastrukturarchitekt
MAN Energy Solutions

gebremst wurde, weil der Anwendungszugang über veraltete VPN-Lösungen mit steigenden Kosten für Appliances, Software und MPLS-Networking erfolgte. Darüber hinaus wollte das Unternehmen Sicherheitsvorteile erzielen, indem Applikationen im Internet unsichtbar gemacht wurden.

„Wir ließen eine verteilte, mobile Belegschaft über ein traditionelles VPN zu erkennbaren Zugangspunkten auf Anwendungen zugreifen. Darunter litt die Leistung. Unsere Mitarbeiter waren unzufrieden mit ihrer Erfahrung.“

Unsere Sicherheitsstellung schöpfte ihr Potenzial nicht aus. Dies war unvereinbar mit dem, was unsere AWS- und Azure-Deployments leisten konnten“, sagte Tony Fergusson, IT-Infrastrukturarchitekt bei MAN. „Außerdem haben wir ein relativ kleines Betriebsteam, das die Infrastruktur vor Ort verwaltet, während unser Datensatz und der Bedarf an Echtzeitanalytik und Anwendungszugriff explodierten. Dies alles zu bewältigen wurde immer schwieriger, als wir unsere internen Anwendungen modernisierten, mehr Datenquellen online stellten und weltweit fortschrittliche Produkte und Technologien einsetzten.“

Warum Zscaler

Für MAN Energy Solutions (MAN) bot der Wechsel zur Cloud klare Vorteile bei der Bewältigung geschäftlicher Herausforderungen. „Wir sahen immer mehr Unternehmen, die Anwendungsfälle mit globalem Umfang erfolgreich in der Cloud implementierten, und wir haben Architekturansätze gefunden, die unseren technischen Zielen entsprechen“, sagt Fergusson.

MAN wandte sich 2011 an Zscaler, um die Nutzererfahrung zu verbessern, die Bandbreitenkosten zu senken und den steigenden Sicherheitsansprüchen gerecht zu werden. MAN begann damit, weltweit verteilte Benutzer mithilfe von Zscaler Internet Access (ZIA) mit den SaaS-Anwendungen des Unternehmens zu verbinden. Später wurde Zscaler damit beauftragt, das Problem von Advanced Persistent Threats (APT) anzugehen. Als nächstes wurde Zscaler Private Access (ZPA) gewählt, um mobile Belegschaft und Auftragnehmer jederzeit von überall aus auf vor Ort ausgeführte Applikationen zugreifen zu lassen. Vor kurzem wurde ZPA für den sicheren Zugang zu Applikationen auf AWS und Azure eingeführt, wodurch die Erfahrungen der Mobilnutzer verbessert und die Netzwerkkosten gesenkt werden.

Zero-Trust-Zugang zu internen Anwendungen

Zscaler Private Access (ZPA) bietet einen auf Richtlinien basierten, sicheren Zugang zu Anwendungen und Assets ohne die Kosten, die Komplexität und die Sicherheitsrisiken eines VPN. Die Idee, interne Anwendungen für nicht autorisierte Benutzer zu „verdunkeln“, hat seit der Einführung des Software Defined Network (SDN) an Dynamik gewonnen. Mit dem Ansatz des Zero-Trust-Modells werden Ihre Dienste unsichtbar. Sowohl Applikationen als auch Benutzer müssen mittels SAML autorisiert sein, bevor Zugang gewährt wird.

VORTEILE

- Vermittelt Endnutzern eine bessere Erfahrung
- Reduzierte Angriffsfläche durch Anwendungszugriff ohne Zugang zum Netzwerk
- Ermöglicht weltweit starke Authentifizierung und granulare Zugangskontrollen für Anwendungen
- Bereitstellung, sicherer Zugang und Verwaltung von VPCs
- Gewährleistet einen optimalen Pfad zwischen Benutzern und Applikationen für eine höhere Leistung
- Größere Transparenz von Anwendungen und Benutzer-Aktivitäten

„Wir waren in der Lage, ein Zero-Trust-Modell einzuführen, oder was ich **Blackcloud (SDP)** nenne“, sagte Fergusson. „Wir haben unsere Lösung implementiert, um unsere Angriffsfläche zu reduzieren, und traditionelle Ansätze durch diese moderne, sichere Cloud-First-Lösung ersetzt. Wir können unsere Benutzerberechtigungen granular kontrollieren, sodass jeder Mitarbeiter und Auftragnehmer nur auf das zugreifen kann, was er benötigt.“

Dieser Ansatz verhindert auch die laterale Bewegung schädlicher Software. Es wird sichergestellt, dass der Zugang nur von einem Client zu einem Server initiiert wird und niemals umgekehrt. Die Kombination dieser beiden Paradigmen verhindert schädliche laterale Bewegung, indem alle Sitzungen vor der Zugangsgewährung validiert werden. Mithilfe eines Zero-Trust-Modells und der

Durchsetzung von Richtlinien, die auf Authentifizierung von Benutzern, Autorisierung sowie bekannten und unbekanntem Anwendungen basieren, wird somit eine höhere Sicherheit erzielt.

Ein moderner Ansatz, um Benutzer in globalem Umfang zu verbinden

Es gab eine Reihe von Geschäftsfaktoren, die eine schnellere, sicherere Art der Verbindungsherstellung zwischen Benutzern und ihren Applikationen erforderten, darunter die Migration von internen Geschäftsanwendungen und Entwicklungsprojekten in die Cloud, die verstärkte Einführung von Cloud-Diensten sowie die Notwendigkeit, einer wachsenden Anzahl von weltweit verteilten Mitarbeitern und Partnern Zugang zu gewähren. Dies erhöht zwar die Geschäftsflexibilität und -agilität, würde bei Weiterverwendung traditioneller VPN-Ansätze aber auch zu einer größeren Belastung von IT- und Netzwerkressourcen führen.

Die Zscaler-Cloud bietet eine elegante und leistungsstarke Alternative. Sie macht herkömmliche Hardware- und Software-Security-Stacks für den Remote-Access sowie die Verwendung eines VPN-Client und Remote-Access-Heuristik überflüssig und stellt einen alternativen Pfad für den Traffic bereit. Dies reduziert den Bedarf an MPLS-Tunneln für Internet-basierte Konnektivität.

Erzielen von Geschwindigkeit, Agilität und Leistung

MAN Energy Solutions verbesserte die Endnutzenerfahrung und reduzierte gleichzeitig Komplexität und Kosten. Endnutzer erhalten nun beim Zugriff auf interne Anwendungen eine völlig nahtlose Erfahrung auf Cloud-Niveau, unabhängig davon, ob die Anwendungen im Rechenzentrum oder in der Cloud ausgeführt werden. Benutzer greifen über die globale Zscaler-

Cloud direkt auf Anwendungen zu, wobei herkömmliche Engpässe beim Remote-Access vollkommen umgangen werden. Dies sorgt für absolute Flexibilität in Bezug auf den Ort, an dem Anwendungen gehostet werden, und schützt sensible Daten mittels einer TLS-basierten verschlüsselten Mikrotunnelverbindung. Benutzer erhalten niemals Zugang zum Netzwerk, Anwendungen werden niemals für nicht autorisierte Benutzer freigegeben und die Cloud reduziert die bei herkömmlichen Lösungen übliche Komplexität.

Durch den Wegfall von VPN-Infrastruktur und Softwarelizenzierung konnten Kostensenkungen im zweistelligen Prozentbereich erzielt werden. Darüber hinaus wurde die Netzwerkleistung gesteigert, indem Bandbreitenkontrollen zur Priorisierung von geschäftskritischem Traffic gegenüber weniger wichtigem Traffic wie Web-Browsen eingesetzt wurden.

Einer der wichtigsten technischen Vorteile besteht darin, dass das Team die Angriffsfläche reduzieren und die gesamte Verwaltung in AWS und Azure sichern konnte. MAN verwendet das Protokollierungs- und Analytik-Cluster von ZPA, um Logs zum eigenen SIEM zu streamen und so einen besseren Einblick in den Zugang und die Aktivität von Benutzern zu erhalten.

„Wir können jetzt innerhalb von Minuten neue VPCs einsetzen und neue Namensbereiche erstellen. Die Verwendung von Namensbereich-Routing ist ein großer Vorteil für uns, da wir den Traffic nun auf Basis von Namensbereich statt IP kontrollieren können. Dies ermöglicht es uns, aussagekräftige Richtlinien festzulegen. Wir können Kosten und Komplexität des Netzwerks senken. Unser beratender Onboarding-Prozess ist viel schneller. Wir können nun innerhalb von Stunden statt Wochen einstellen“, ergänzte Fergusson.

Über Zscaler

Zscaler wurde im Jahr 2008 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.

